1. INTRODUCTION

This document provides a general overview of CenturyLink’s Information Security Framework and details CenturyLink’s information security principles that cover all standard CenturyLink services including cloud infrastructure and hosted IT data, voice and managed services solutions.

CenturyLink’s Information Security Framework encompasses all forms of information or data handled by CenturyLink, including CenturyLink proprietary data and data handled on behalf of CenturyLink’s commercial, corporate, and government customers.

CenturyLink’s Information Security Framework is designed to protect CenturyLink information assets from threats, whether internal or external, deliberate or accidental. This Information Security Framework document recognizes the importance of information to CenturyLink and establishes steps to be taken to help protect its confidentiality, integrity, and availability.

1.1 Purpose

This document provides customers with an overview of the applied methodologies and security aspects within CenturyLink, including the security focus areas listed below:

- CenturyLink Information Security Policies, Guidelines and Procedures
- ISO 27001:2013
- Generally Accepted Audit and Compliance Standards
- People
- Physical Security
- Information Security
- Operational Management
- Compliance Management

A limited number of CenturyLink services in certain locations are provided out of third-party data centers rather than CenturyLink data centers. CenturyLink reviews such third party’s security controls, compliance programs, and audit reports at least annually.

1.2 Scope Statements

This document covers CenturyLink information, data, and assets and requirements that are applicable to all employees and contractors of CenturyLink and its affiliates. This Framework may not apply to customized or other non-standard services, configurations, or environments.
CenturyLink information, data, and assets must be protected and as such, reasonable measures are taken during the installation and configuration of all internal infrastructure, external infrastructure, and third-party connections to ensure the integrity and privacy of CenturyLink’s information. CenturyLink limits its reliance on access/authorization control mechanisms at any third-party site to protect or prohibit access to CenturyLink’s confidential information. All third-party connections are reviewed on a periodic basis and any changes or updates regarding those connections will be handled as necessary.

All employees are obligated to safeguard the confidentiality, integrity and availability of the information, data, and CenturyLink information systems at all locations. All employees and agents of CenturyLink who have access to or custody of information, data, and information systems are required to understand and comply with any and all policies, standards and guidance established to support the Information Security Framework.

CenturyLink services are designed to address information security controls to protect customer information assets. In this way, current and prospective customers may find that CenturyLink provides them with valuable tools in implementing their internal and regulatory compliance programs. Customers may leverage any of CenturyLink’s security services to deploy multiple or varying layers of security to best suit their needs.

The physical and logical integrity of all data center systems is important to making sure customer infrastructure remains secure. CenturyLink follows industry accepted security best practices including defense in-depth and layered security controls in order to monitor and detect security events and to protect the information and data stored on CenturyLink information systems.

2. CORPORATE ETHICS

CenturyLink is committed to conducting business in accordance with the CenturyLink Unifying Principles and has established Corporate Ethics policies designed to communicate the ethical and legal standards that govern our business conduct. The CenturyLink Code of Conduct, Anti-Corruption Policy, and the Business Courtesies Policy apply to all CenturyLink employees. Please see http://www.centurylink.com/Pages/AboutUs/Governance/ethics.jsp for more information regarding these policies.

**Code of Conduct**

The CenturyLink Code of Conduct outlines the standards of conduct that apply to all company employees, including executive officers, and provides extensive and detailed guidelines and ethical standards.

**Anti-Corruption Policy**

The Anti-Corruption Policy provides guidance for compliance with anti-corruption laws including, but not limited to, the U.S. Foreign Corrupt Practices Act and the UK Bribery Act. CenturyLink employees have two primary obligations under this policy: (1) never accept, offer or pay a bribe, facilitation payment, or kickback; and (2) always accurately reflect transactions in the company’s books and records. A copy of this policy can be made available upon request.
Business Courtesies Policy

The Business Courtesies Policy provides guidance for offering or accepting business courtesies e.g., gifts, meals, or entertainment. As a general rule, CenturyLink employees must determine whether any business courtesies offered or accepted are:

- Reasonable in value
- Infrequent
- Related to a legitimate CenturyLink business purpose

Moreover, as explained in the policy, employees must seek written pre-approval from Corporate Ethics and Compliance before offering any business courtesy to a local, state, federal or foreign (non-U.S.) government official or family member of a government official. A copy of this policy can be made available upon request.

3. ISO 27001:2013

The ISO27001:2013 Information Technology - Security Techniques - Information Security Management Systems - Requirements document establishes the guidelines and general principles that CenturyLink uses for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system (ISMS) for Managed Hosting services, Global Network services and Global Colocation services. The objectives outlined provide general guidance on the commonly accepted goals of information security management and standard practices for controls in the following areas of information security management:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Communications security
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance
- Cryptography
- Supplier relationships

3.1 Overview

ISO 27001 has been implemented as the structural foundation for CenturyLink's Information Security Program and Policy. This approach assists senior management in their obligations to monitor and control security, thereby reducing risks to both CenturyLink and its customers. The ISMS is designed to select adequate and proportionate security controls to protect information assets.
CenturyLink uses the ISMS to address the following:

- Formulation of security requirements and objectives
- Cost-effective management of security risks
- Compliance with laws and regulations
- Process framework for the implementation and management of controls to meet specific security objectives of the organization
- Identification and clarification of existing information security management processes
- Status of information security management activities
- Internal and external auditor reference
- Relevant information about information security policies, directives, standards and procedures to appropriate parties

Additionally, CenturyLink holds ISO/IEC 27001:2013 certification specific to the ISMS supporting CenturyLink’s global network services and managed services as well as CenturyLink’s global colocation services.

### 3.2 Responsibility

CenturyLink information security responsibilities are aligned with Corporate Security, which is managed by the designated Chief Security Officer (CSO). All CenturyLink employees are responsible for adhering to all policies, standards and guidance established to support the CenturyLink security program. CenturyLink employees are responsible for recognizing, alerting, responding to, and reporting any incident, outage, or activity that could be harmful to CenturyLink’s information systems.

Each business unit is accountable to implement and enforce this framework as it applies to the information handled and information systems managed in its scope of responsibility.

While CenturyLink employees are required to protect customer data with which they come in contact while providing support to our customers, it is the customer’s responsibility to provide the appropriate security measures to ensure protection of their network, environments, information, and data.

### 3.3 Audits

The information security framework requires that external audits of CenturyLink corporate systems and infrastructure are conducted at least annually. Additionally, critical systems in the Managed Hosting and Colocation environments are audited quarterly. Audit levels and details correspond to the level of risk assessed for each system. Members of the CenturyLink cybersecurity team may also conduct internal spot audits whenever new risks are identified, or at any other time deemed necessary.

Cybersecurity team members may also, if necessary, conduct network and host-based audits of CenturyLink corporate Infrastructure and IT systems as needed to address zero-day or newly discovered exploits without prior notice.
4. POLICY & PROCEDURES

Some business units have separate policies, specific to the business unit, which are separately maintained due to legacy contractual and compliance requirements. Policies specific and relating to information security are considered extensions of the CenturyLink Information Security Policy and are reviewed at least annually, or as needed, and amended to reflect changes in requirements, technology, and other circumstances. Policy violations are subject to appropriate disciplinary action up to, and including termination of employment.

4.1 Data Center Colocation and Managed Services (DCCLMS) Policies

CenturyLink has implemented the *Information Security Policy* and supporting methods and procedures, technical standards, and processes to reinforce the importance of information security throughout the organization.

DCCLMS policy documents are approved by the Chief Information Security Officer (CISO) and outline the requirements to maintain effective security within data centers, specific to colocation and managed services environments. The implementation of these policies provide DCCLMS and CenturyLink increased security awareness and reduced risk exposure. These include, but are not limited to the following:

- Physical Security Policy for Data Centers and Office Locations
- Electronic Use Policy including:
  - Email Usage
  - Wireless Networks
  - Internet Access
  - Anti-Virus control
- Password Management
- Remote and Home Working
- Computer Security Incident Response Plan
- Information Protection
- Third Party Connections Agreements
- Third Party Access
- Wireless Scanning
- Risk Management
- Vendor Management

4.2 DCCLMS Procedures

CenturyLink uses DCCLMS procedures and guidelines to help maintain a secure environment. This requires DCCLMS to implement procedures that include, but are not limited to:

- Anti-virus
- Incident handling
- Change Control
- Access Control
- Wireless Networks
- Remote Working
- Third-Party Connection Management
- Third-Party and Visitor Access
These procedures contain guidelines which help to ensure consistent business activities that are compliant with the policy, including:

- Clearly defined employee responsibilities regarding:
  - Data Protection
  - Use of email, Internet and telephones
  - Incident management
  - Security of buildings, equipment and personnel
- Specific requirements for the following:
  - Connection of devices to DCCLMS networks or resources
  - Rules to be applied for passwords and password protection
  - Access to DCCLMS facilities by visitors

5. PEOPLE

5.1 Recruitment

To maintain the integrity of hired employees, CenturyLink has implemented a recruitment policy that covers, but is not limited to, the following:

- Comprehensive interview process
- Validation to confirm that new employees have the qualifications represented
- Reference and work history verification

In some cases, expanded vetting may be undertaken to address specific business or customer requirements.

5.2 Background Checks

Once appropriate written authorization from prospective employees has been secured, CenturyLink performs a background screen that includes verification of prior employment, and verification of education. For prospective employees for positions requiring access to client information, whether physical or logical access, CenturyLink performs a criminal records search for the prospective employee’s current county and state of residence prior to allowing access to the client information.

For employees in the United States, CenturyLink also verifies the employee’s status to rightfully work in the US through compliance with the Immigration and Naturalization Service’s I-9 process (I-9 Check).

For employees in jurisdictions outside the United States, CenturyLink verifies that prospective employees comply with local law requirements with respect to the right to work in such jurisdictions.

Furthermore, for CenturyLink employees in the U.S. who are applying for security-sensitive positions (including Security Operations Center personnel), CenturyLink performs a criminal conviction screening through an authorized background-reporting agency, prior to granting access. The background screen covers a seven (7) year time period and includes all locations in which the employee resided during that period.
Additionally, the background screen includes a Government List Screen, which covers the following lists published by the US government:

- Department of State, Arms Export Control Debarment List
- Department of State, Proliferation List
- Department of Commerce, Denied Parties List
- Department of Commerce,Entities List
- Department of Treasury, Specially Designated National List

For CenturyLink employees providing security sensitive services in jurisdictions outside the United States, and in the event that local law does not permit CenturyLink to perform a full Background Screen, CenturyLink performs background screening to the extent permissible under local law.

5.3 Drug & Alcohol Abuse

CenturyLink fully endorses the requirements of the Federal Drug-Free Workplace Act. It recognizes that alcohol and drug abuse pose potential health, safety and security problems. Employees are expected and required to report to work on time in appropriate mental and physical condition for work. CenturyLink has adopted the Drug and Alcohol-Free Workplace Policy which prohibits:

1. Impairment by legal medications or alcohol while working, while on CenturyLink premises, in CenturyLink vehicles, or at sponsored events;

2. The use of alcohol in excess or to the point of intoxication while attending any company-related or company-sponsored events, regardless of whether such events are on or away from company premises. Drinking alcohol in moderate quantities on CenturyLink premises or at sponsored events is permissible with VP approval (though good judgement is always expected); and

3. The use, possession, sale, manufacture, distribution and/or being under the influence of illegal drugs/controlled substances, possession of drug-related paraphernalia while on company premises, while performing duties for CenturyLink while away from company premises, or while attending CenturyLink-related events and/or during working hours.

The substances prohibited by this policy include such items as any illegally or unlawfully obtained drugs or controlled substances, designer or synthetic drugs, over-the-counter or prescribed medications not being used for the purposes or in the manner intended, and non-prescription mood or mind-altering substances.

Compliance with this policy is required by CenturyLink as a condition of employment for qualified applicants or for continued employment of current employees. The presence of any detectable amount of any prohibited substance in an employee while working and/or during working hours may be deemed a violation of this policy, regardless of when or where the substance entered the employee’s system.
Testing of CenturyLink Employees

Except as otherwise required or prohibited by law, an employee will be subject to testing in the following circumstances:

(1) When an employee’s conduct, actions or behavior reasonably leads management, in consultation with Human Resources, to suspect that the employee may be using or under the influence of illegal drugs or alcohol in violation of the policy.

(2) When an employee has a prohibited substance in his or her possession (actual or constructive) while on CenturyLink premises or while performing duties for CenturyLink while away from company premises and/or during work hours; and

(3) When an employee has experienced an on-the-job injury or accident or is involved in an incident which CenturyLink believes may have resulted from impairment due to drug or alcohol use.

5.4 Terminations

CenturyLink Human Resources (HR) personnel notify a member of the security team as soon as possible in advance of all voluntary or involuntary employee terminations, so that network accounts can be terminated, and other necessary preparations or precautions can be taken in a timely fashion. When the company terminates an employee, a security team, HR, or other designated representative should be present with the manager to escort the person to collect their personal belongings and leave the premises immediately.

A terminated employee shall not be permitted to access any computer systems or remain unescorted on the premises once notification has been made, except under unusual conditions, and with explicit permission granted by the company vice president and approved by security staff, who may impose additional restrictions.

5.5 Security Awareness

Every CenturyLink staff member is required to annually complete information security awareness training. Participation is obligatory and is managed by departmental heads and Human Resources with acknowledgement of completion by each individual. The Information Security Awareness training program includes: user ID and password best practices, information classification, personally identifiable information (PII), Payment Card Industry (PCI), protected health information (PHI) requirements, and legal and regulatory requirements.

5.6 Compliance

Non-compliance with the CenturyLink policies by employees or designated agents will be subject to management investigation and disciplinary or other action, which may include termination.

5.7 Confidentiality

CenturyLink believes that information is one of the company’s most valuable assets and is integral to our products and services. That makes information security of paramount importance because handling and protecting it in a responsible manner creates a trusting relationship with our customers. Furthermore, maintaining the confidentiality and integrity of our information is essential to complying with legal and regulatory requirements.
All CenturyLink employees are required to complete a yearly review and acknowledgement of CenturyLink’s Code of Conduct, CPNI, and Security Awareness training, all of which describe the importance of safeguarding proprietary and confidential information from disclosure. This obligation to protect CenturyLink proprietary and confidential information extends beyond employee termination.

5.8 Professionalism

All CenturyLink employees are selected for their experience and knowledge. Some examples of the employee qualifications include certification from vendors and well-known organizations, such as:

- ISC2
- ISACA
- Cisco
- Microsoft
- SANS

Additionally, CenturyLink has a formal training department with sufficient budget to encourage further employee growth and career development.

6. PHYSICAL SECURITY

6.1 Responsibility

The CenturyLink Global Data Center Physical Security and Physical Security organizations have global responsibility for all physical security operations, security systems, access administration, and security controls within all CenturyLink-owned facilities and data centers. Third-party data centers are utilized for certain services and, in such cases, are not considered CenturyLink-owned data centers.

CenturyLink Corporate Security has implemented security policies to reinforce the importance of physical security of all company facilities including procedures specific to data center physical security. Each CenturyLink data center has a Security Operations Center (SOC) or security desk. Data center security personnel are responsible for controlling data center access, monitoring local security alarms and closed-circuit television (CCTV) cameras, and managing all physical security-related events reported by the SOC.

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 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 CenturyLink access badges and administration of access permissions within the access control system.
6.2 Data Center Access

CenturyLink utilizes mantrap portals that require two-factor authentication controlling access to the front entrance of the data center. Man traps are used to prevent tailgating. Two-factor authentication is also required prior to entry to the raised floor areas of the data center.

All persons requesting access into a CenturyLink data center must verify their identity by presenting valid government-issued photo identification or a CenturyLink-issued photo access badge. There must also be a valid reason presented for requesting access.

All persons are to enter and exit the data center through the authorized entrances only. Customers and their authorized representatives are not to enter or exit the data center through any other building exits, including the loading dock and service exits. Emergency exits are to be used only in the case of a fire or life safety emergency.

6.3 Access Control Systems and Badges

The CenturyLink Access Control System (ACS) utilizes access badges in conjunction with 2-factor authentication to restrict access to only those individuals with proper authorization.

All persons entering the raised floor 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 visible at all times. 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.

Access badges remain active until the badge holder’s authorization is revoked. Customer badges will automatically become inactive if not used for more than ninety (90) consecutive days. The badge holder may request re-activation on their next visit to the data center.

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. 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 them when departing the data center or facility.

The CenturyLink Facility Access Control System (FACS) is used to manage and document permanent badge issuance. The FACS is used for new access badge requests and for the renewal, deactivation, replacement or change of an existing badge. All requests for badge access to affiliated data centers must be submitted and approved through FACS by the requestor’s sponsor/manager and the designated data center site authorizer prior to the badge being issued.

All access control records are available online for 90 days. Events beyond 90 days are archived and stored offline for a minimum of two years.
6.4 Video Surveillance

CenturyLink-owned data center premises are under 24-hour closed circuit television (CCTV) video surveillance. CCTV systems are designed to cover the exterior and common interior spaces of the data center, including raised floor ingress/egress points.

CCTV provides facial recognition for all persons entering the raised floor area of a data center as well as other restricted areas such as node rooms, power rooms, managed cage areas, etc. Customer colocation space is not included within CenturyLink CCTV surveillance. All CCTV systems are configured to retain 90 days of recorded video.

Customers may provide and install video surveillance equipment within their colocation space, but such systems must be approved by CenturyLink prior to installation and comply with certain restrictions, which are subject to change from time to time at CenturyLink's sole discretion. Customer-owned cameras must be positioned so that only their equipment is being monitored to protect the privacy and activities of other CenturyLink customers. Customer-provided video systems are subject to inspection and periodic unannounced audits to verify compliance.

6.5 Customer Access

CenturyLink colocation customers are responsible for providing and maintaining an accurate listing of their employees, contactors, and vendors authorized for access into the 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 SavvisStation Portal. The customer’s authorized personnel are listed as an active contact under the customer site record with permanent or temporary data center access permissions for the specified data center.

Only persons designated by the customer as a “Contact Administrator” with administrative-level permissions within the portal may add, change, or delete active contact records, and add, change, or remove data center access authorizations to an active contact record. The CenturyLink Global Operations Center service analysts, including the Colocation Support Group, and/or CenturyLink account support representatives may also manage access authorizations for the customer.

**Note:** Customers may only authorize access to data centers where they receive active colocation services from CenturyLink. Access authorization may be granted on a permanent or temporary basis to any active customer contact. Persons requiring access to more than one data center must have separate access permissions for each data center assigned to their contact record.

Contact administrators may revoke access authorizations at any time by removing data center access permissions from an active contact or simply making the contact inactive. In the event a customer discontinues their colocation services with CenturyLink, all related data center access badge privileges will cease with the stop bill date for such services.

Only persons with approved, permanent data center access are eligible for a CenturyLink customer badge. Persons with temporary data center access permissions are provided a temporary customer badge to be used while in the data center.
Colocation customers are required to have an approved request in FACS for new badges. The customer may submit a customer access badge request within the CenturyLink portal or by filling out a badge application on their first visit to a data center. To qualify for a customer badge, the applicant must be an active contact under the customer site record with permanent access authorization for the data center.

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.

Customers may only access those portions of the data center made available 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, restrooms, and breakrooms) unless otherwise approved and accompanied by an authorized CenturyLink representative.

Customers and their authorized representatives may not enter the Managed Service, Node, and Meet Me Room areas of the data center at any time. Additionally, CenturyLink Cloud data centers are closed to Customers given the virtual architecture of the public platform.

6.6 Employee and Regular Contractor Access

Not all active CenturyLink employees or contractors are authorized to access a data center. Employees and regular contractors must submit a badge request in FACS, and must be approved by their sponsor or manager. Requests that include badge access to a data center must also be approved by the designated data center site authorizer and authorized through the CACC upon approval.

6.7 Visitor Access

A person entering a CenturyLink facility, 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 access badge and current access authorization to the facility or data center.

Authorized sponsors are permitted to escort up to five visitors at one time. 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 a valid (unexpired) government-issued photo identification
- Wear their visitor’s badge at, or above the waist. The badge must be visible at all times 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 in the data center
- 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
- 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

6.8 Property Controls

Adherence to the following property controls is strictly enforced. Security personnel are to report violations immediately to the data center facility staff.

Equipment Removal

CenturyLink prohibits the unauthorized removal of company assets from its premises. Security operations personnel are authorized to conduct inspections of property coming in to or going out of company facilities or data centers.

Prohibited Materials

The following items are prohibited in the data centers:

- Food or drink – prohibited on the raised floor
- Tobacco products (including smokeless) – prohibited on the raised floor
- Paper products (other than equipment manuals) or other combustible materials of any kind, including cardboard and boxes – prohibited on the raised floor
- Explosives, firearms, or weapons of any kind
- Chemicals or Hazardous Materials
- Non-prescribed drugs or alcohol
- Magnets and Electromagnetic devices
- Radioactive materials
- UPS equipment, other than what is provided by CenturyLink
- Photographic equipment or video/audio recording equipment of any kind (unless preauthorized by data center management). Cellular phones and tablets are permitted, but use of the camera or video function is prohibited
- Floor tile pullers (subject to confiscation)

Prohibited Behaviors

The following is a list of activities prohibited in the data center:

- Lifting of floor tiles
- Accessing the area under the raised floor
- Accessing the area above the drop ceiling
6.9 Photography

CenturyLink prohibits the photography, or image capture, of the interior or exterior of any CenturyLink data center facility without prior written authorization.

The use of image-capturing devices with either traditional or digital imaging capabilities are included. 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 at CenturyLink facilities is strictly prohibited.

Persons requesting to photograph or video record at any CenturyLink data center must demonstrate a specific business need which cannot be met without the taking of video or photographic images and, prior to any image capture, obtain written authorization from the relevant Data Center Facilities or Operations manager. Image capture of any areas outside a customer colocation cage/cabinet, directly or indirectly, including without limitation any equipment, facilities, materials, or areas belonging to CenturyLink or any it's other customers, is strictly prohibited.

Any persons found to be engaged in unauthorized photography at a data center must be reported immediately to data center security and/or data center manager for intervention. All persons found with unauthorized photographic records will be requested to destroy or delete the captured images. Failure to adhere to this request may result in the immediate removal of the person from the data center and suspension of their data center access privileges.

Violation of this policy by hosting colocation customers is considered a material breach of their contract with CenturyLink and subject violators to legal action.

6.10 Weapons

CenturyLink strictly prohibits firearms or other form of weapons, including but not limited to knives (other than small pocket knives), explosives (including fireworks), hazardous chemicals, and hazardous devices in company buildings or in company vehicles.

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

6.11 Parking Lot Security

With the exception of multi-tenant facilities, parking is restricted to CenturyLink employees, customers, contractors, and visitors only. All other vehicles are subject to tow at the owner's expense.
Customers and employees are required to park in designated spaces only. Vehicles parked in non-designated areas are subject to tow at the owner’s expense.

Handicapped parking spaces are restricted to those vehicles displaying a current handicapped license plate or hanging placard issued by the state. These spaces are designated with the International Symbol of Access (wheelchair symbol) or a blue curb.

6.12 Use of Social Media

CenturyLink considers the street address and location of most of its data centers to be confidential information to our business which is made available to our customers and suppliers under non-disclosure agreements. While the location of some CenturyLink sites is available through Internet searching, CenturyLink requires that employees, customers, and contractors not use social media to divulge the location or physical address of a data center or any information that is confidential, proprietary, or non-public information.

6.13 Entry and Exit Inspections

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

6.14 Environmental Control

The CenturyLink DCCLMS data centers are equipped with air conditioning, fire suppression, UPS and backup generators, all of which are connected to the building management system, monitored 24/7/365 by operations personnel.

6.15 Third-Party Data Centers

Third-party data centers may be employed for certain services through the course of acquisitions or as pertinent to the technology. Validation of certain physical security and other controls for third-party sites are reviewed annually by CenturyLink.

7. INFORMATION SECURITY

7.1 Network Security

CenturyLink utilizes a defense in depth strategy by implementing multi-layered security starting at the perimeter, using routers and firewalls to protect the network. Additionally, multiple internal intrusion detection systems (IDS) are deployed to monitor the CenturyLink corporate infrastructure for internal or external attempts to circumvent security policy.

CenturyLink DCCLMS manages its customer environments via a unique private network management infrastructure. Management connectivity to the customer equipment is provided through a separate logical channel, which is only accessible from the private CenturyLink DCCLMS management network. Data center customers are also managed through an independent private management network with multiple layers of security applied within the data center and WAN connectivity paths to CenturyLink DCCLMS management infrastructure. Network services are configured restrictively on CenturyLink DCCLMS infrastructure and have appropriate security bug fixes (patches) installed periodically.
For Managed Services customers, CenturyLink DCCLMS notifies customers of new or updated security bug fixes (patches) and will perform risk assessment, schedule changes, and apply patches as necessary. For Colocation customers, as we have limited knowledge of their environment connected to our network, if an issue originating from a customer environment becomes apparent, CenturyLink will notify the customer of the issue and reserves the right to disconnect the customer environment or block addresses until issue is resolved.

7.2 Access Control

The principle of least privilege is adopted by CenturyLink and access is controlled through the following:

- Two-factor authentication before being granted access to systems used for customer server or device management
- No direct access between the CenturyLink corporate IT network and the management network
- Logging of authentication events
- Separation of duties based on a “need to know”

7.3 Anti-Virus

CenturyLink maintains a strict anti-virus policy. All files transferred electronically into the CenturyLink environment must be scanned before, during, or immediately after the transfer. Periodic scans are carried out within the CenturyLink environment to help maintain a virus free environment.

7.4 Password Management

Users are required to log in using their own unique username and password to maintain accountability. Where supported, CenturyLink requires that complex passwords and minimum length requirements are enabled. Systems are configured to ensure periodic password changes. Password history is also tracked to ensure that password reuse is not allowed.

All administrator or root-level accounts on systems are specifically controlled and not utilized except as necessary for escalated privilege operational support.

7.5 Data Classification

Data is classified into three categories, public, confidential, and highly confidential. Each classification has different rules for storing, transferring and destroying data.

7.6 Media Sanitization

Bulk or certified destruction of tape media:

CenturyLink DCCLMS uses a bonded tape archival services vendor, who handles tapes in accordance with stringent CenturyLink specifications. The media is physically destroyed using a FACTA-compliant shredding process. The vendor provides written confirmation specifying the individual serialized barcodes that were destroyed.
Drive Reuse:

For CenturyLink DCCLMS, if storage is released from within the same array, the LUN is scrubbed by writing 0's across the LUN. Once this operation is completed, the storage is returned to the provisioning pool for re-use, thus preventing deployment of old data on new LUNs.

For CenturyLink Cloud, all storage is part of a virtual machine (VM) instance as the VMDK file. When a VM instance is deleted, the storage is released and can and will be overwritten by other actions on the platform.

Managed servers with internal hard drives:

The standard sanitization method used by CenturyLink DCCLMS is a DoD 5220.22-M three pass overwriting algorithm. A certificate of destruction can be requested from CenturyLink personnel and is available for a fee.

For CenturyLink Cloud, this isn't relevant within a VM environment. However, there is a procedure for how data destruction is handled in the cases of hard drive failure/replacement and/or server relinquishment for Bare Metal servers. All local storage associated with Bare Metal servers is fully encrypted. As such, destruction is not necessary to protect sensitive data. New encryption keys are automatically generated for each newly provisioned server. Encryption is controlled exclusively by the disk array controller and not within the OS or elsewhere. CenturyLink Cloud controls the encryption keys and each key is tied directly to the logical volume on the array controller. When the logical volume is deleted there is no recovery path as the associated key is destroyed at the same time by the array controller. Thus, the data is rendered unrecoverable as part of our routine rediscovery and provisioning process for servers being decommissioned.

8. OPERATIONAL MANAGEMENT & CONTINUITY

8.1 Incident Management

CenturyLink provides customer support 24 hours per day, seven days per week. When an incident has been detected or a customer request is received, CenturyLink uses commercially reasonable efforts to meet the time to respond objectives (TRO) we have in place.

CenturyLink's Cybersecurity Incident Response Team (CIRT) has an incident response process which is followed when a suspected security incident has been either detected or reported by a customer. The incident response process contains a procedure which is followed to help classify the security incident as well as the steps necessary for handling the incident based on its classification and for engaging other organizations as appropriate.

CenturyLink classifies every information security incident into one of many categories, which is then specified within an associated security incident ticket. The classification of an incident may change during the incident handling process as more information becomes available.
8.2 Incident Remediation/Recovery

CenturyLink defines Incident Remediation/Recovery as the capability to recover from information security threats/incidents pertaining to the CenturyLink Enterprise environment after incident response/containment has been completed. Remediation and recovery steps include follow-up actions that protect the compromised system/data from future similar attacks.

In the event of an incident requiring remediation/recovery, the following tasks and responsibilities are implemented by CIRT:

- Provide oversight to validate proper countermeasures and controls have been implemented to avoid a future compromise of similar nature.
- Notify and engage key parties and resources to support remediation/recovery efforts.
- Develop, document, and distribute Incident Response guides with remediation procedures as needed.
- Ensure any vulnerable systems discovered during threat investigation become remediated and compliant to CenturyLink Corporate Security standards.
- Engage other security teams such as Security Vulnerability Assessment, Compliance and Audit, Architecture and Engineering, etc. to assist with other security measures as needed.
- Develop/deploy scripts, tools, and systems to improve threat detection and response capability.
- Engage CenturyLink Legal for breach disclosures to external organizations and customers as needed.
- Document remediation/recovery actions within a security incident ticket.
- Create formalized Incident Response Report on significant incidents.

8.3 Patch Management

The patch management service that CenturyLink provides to customers is a mature process strengthened by years of providing managed hosting and application services to our clients. CenturyLink has implemented automated patch scanning of servers to keep servers up to date with the latest software and security fixes.

CenturyLink updates managed servers with vendor recommended security patches, service packs, and hot-fixes and will address the overall integrity and performance of servers throughout the life of the hosting solution. This allows CenturyLink to maintain a consistent, controlled environment to help minimize unforeseen costs and downtime.

Our validation process helps ensure compatibility, stability, and performance. CenturyLink’s Cyber Defense organization actively participates in industry forums, communities, and initiatives to keep abreast of the latest security threats and vulnerability alerts, often times before they are widely announced to the public.

All hot-fixes and non-security related patches are evaluated for impact and urgency and follow the same testing and integration guidelines as service pack upgrades. If a reboot is necessary to complete the installation of the patches, CenturyLink will endeavour to conduct this during maintenance hours or coordinate these activities with the customer.
The customer must approve patches or service pack upgrades that may impact their applications, prior to them being applied to their servers. Such situations are addressed on a case-by-case basis. Failure to apply required patches / fixes / services packs may affect the service level agreements associated with the supported services. In addition, CenturyLink will work with the customer to confirm that patches are first installed and tested on their test/QA environment prior to installation to production servers and determine that customer applications continue to function appropriately.

8.4 Change Control

CenturyLink uses the ITIL approach to service management including a mature change management process.

The CenturyLink DCCLMS Change Management policy is designed to apply standardized methods and procedures on a global basis to provide efficient and prompt handling of all changes to the CenturyLink infrastructure and to minimize the impact to CenturyLink customers. This process enables rapid deployment of changes within the customer’s system environment using highly defined and controlled processes to maintain system integrity.

Objectives of the Change Management process include:

- Enabling the continuity of business and system processing
- Establishing a process for communicating and managing changes for increased visibility to both the business and operational support staff
- Allowing for mutual impact assessment and resource planning to manage scheduled changes
- Reducing the number of incidents caused by changes
- Increase effectiveness of changes by including lines of business in the decision process
- Improve confidence in the Global Technical Organization to maintain network and system availability
- Accurate and effective prioritization of requested changes
- Ability to absorb a high level of change without difficulty

Definition of a Change - For the purposes of this process, changes are defined as additions, modifications or deletions of any service, hardware or software component within a customer’s environment managed by CenturyLink. Examples of change include but are not limited to:

- Hardware adds, changes and moves
- System software changes (operating level)
- Application changes (e.g. functional updates, significant updates that require new or additional infrastructure such as disk, processing or network bandwidth)
- Network changes
- Interface changes
- Database changes
- Version upgrades / enhancements / patches
8.5 Risk Management

The Risk Management Program is designed to address risks that could impact CenturyLink’s Global Data Center Colocation and Managed Services (DCCLMS) and does not encompass Enterprise Cloud and IT Solutions. Risk Management Framework provides oversight for the management of risks and internal controls associated with the following:

- Product
  - Colocation (security, network, power)
  - Managed Services (security, network, power, managed hardware, application and monitoring services)

- Data Center Locations
  - Domestic US
  - International, APAC, EMEA

The CenturyLink DCCLMS Risk Management Program (internal and external) is organized into 8 main areas:

1) Ethics and compliance
2) Privacy and records management
3) Physical and information security
4) Safety and environmental management and disaster preparedness
5) Asset management – Confidentiality, Integrity, and Availability (CIA)
6) Human Resources
7) Operations
8) Sales/Client Services

8.6 Business Continuity

In today’s global information age, we recognize that unexpected situations may occur and may impact an organization’s operations limiting its ability to deliver services to end users (e.g., customers, field offices, governmental agencies, and the public). CenturyLink has pre-determined and pre-established recovery strategies to maintain a resilient continuity state for its own vital infrastructure to provide for the swift and seamless recovery of CenturyLink systems, with minimal disruption to its own internal operations.

CenturyLink management is committed to maintain resilience of critical infrastructure by conducting periodic testing as jointly directed by CenturyLink’s corporate Information Security, Engineering and Compliance Management departments. Recovery strategies receive ongoing reviews to evaluate current and future risk in order to maintain appropriate procedures and responses. The CenturyLink Disaster Preparedness Whitepaper is available to customers in good standing with an NDA in place.

CenturyLink has implemented a straightforward strategic approach toward recovery. Strategies are designed to handle high-impact, unforeseen business disruptions varying in length and scope, where each CenturyLink facility is capable of recovering CenturyLink identified functions according to their critical timeliness.
The CenturyLink strategy is comprised of the following components:

- Identification of CenturyLink’s mission-critical systems, related recovery objectives, and backup systems
- Review of CenturyLink’s financial and operational risk
- Employee safety and communications
- Alternate recovery site and preparedness for CenturyLink critical systems
- Manned and electronic security management and managed network security verification at all CenturyLink facilities
- Customer notification preparedness through pre-determined event management protocols

The CenturyLink strategy is based on the best practice guidelines of currently recognized business continuity standards and utilizes business continuity professionals to manage the business continuity management program.

As the building blocks toward mitigating the risk and the impact of a potential outage, the CenturyLink strategy is designed to restore operability of its targeted systems, applications, and facilities in the event of an outage or emergency with the following elements in conjunction with the above items:

**Resilient Network Infrastructure:** The main goal is to withstand any single physical fault that occurs on CenturyLink long haul circuits (intercity trunks), short hauls (connecting PoPs within a city), central processor cards, input / output processor cards, fans, power supplies, power grids and HVAC. The CenturyLink network is built with particular attention to redundancy, diversity, and fault tolerance for CenturyLink critical systems and infrastructures.

**Hardened Data Center Facilities:** CenturyLink operates staffed and electronically secured data centers located in the US, EMEA, and APAC. Each data center maintains specific protocols for emergency and disastrous situations and conditions. Mandatory structural (in California this also includes seismic bracing) along with mechanical, utility, and Fire/Life/Safety systems are in place to provide adequate levels of security and recovery.

**Notification to Customers:** Systems have been pre-determined to address conditions surrounding an outage that may impact various CenturyLink services. CenturyLink maintains decentralized and geographically deployed CenturyLink Service Centers (SCs) to handle communications both internally and externally in order to maintain quality and SC availability.

Each of these integrated processes reinforces the essential organizational framework safeguarding against natural, technological, and human error events. Key management and technical personnel are also available 24/7 to service and maintain CenturyLink’s critical systems and functionality.

**Customer’s obligations:** It is the customer’s responsibility to develop, implement, identify, and maintain their own Business Continuity or Disaster Recovery (BC/DR) policies to meet their organizational or regulatory requirements. CenturyLink’s business continuity strategies are solely intended for its own internal infrastructure and are not intended to replace any customer specific BC/DR plan to satisfy any BC/DR planning requirements.
CenturyLink does not guarantee that CenturyLink’s Business Continuity and Recovery Strategy will adequately address all disasters or emergencies, including regional blackouts, natural disasters, pandemic disease outbreaks, terrorist attacks or other crises of a local, national or international scope, or that the CenturyLink data centers or the services it provides will not be impacted by such disaster or emergency conditions. Customers may engage CenturyLink Professional Services consultants to design and implement contingency programs if they desire.

**Pandemic Disease Outbreak**

CenturyLink maintains contingency plans to provide for employee resource planning which may be associated with any disaster including pandemic outbreaks.

CenturyLink’s business continuity plans enable the company to respond to a myriad of disaster-related impacts to include site closures, technology and infrastructure failures, external vendor/contractor disruptions, employee impacts, pandemics, and others as a part of all-hazards planning.

CenturyLink has incorporated into its business continuity planning a methodology to address potential or significant disruptions in employee staffing levels. Additionally, CenturyLink has a comprehensive wellness program that includes influenza vaccinations at no-charge to employees.

With respect to pandemic disease outbreaks, CenturyLink will contact the World Health Organization (WHO) and Center for Disease Control (CDC) and follow their guidance on how to prepare and/or address situations as they may arise.

9. **COMPLIANCE MANAGEMENT**

CenturyLink has a formally designated Compliance Management team to support and facilitate global compliance programs for certain services, including PCI-DSS, SSAE 16 SOC 1 and SOC 2, HIPAA, ISO 27001, and FedRAMP audit programs. Additional compliance support is provided for Business Continuity and Disaster Recovery and Global Risk Management. The compliance programs listed below are specific to Data Center Colocation Managed Services unless otherwise noted.

9.1 **SSAE 16 (SOC 2 and SOC 3)**

CenturyLink Cloud operations are currently audited in accordance with AT Section 101, Attestation Engagements, of SSAEs and publishes a SOC 2 and SOC 3 report for the period July 1 through June 30.

The business unit formerly known as Savvis/CenturyLink Technology Solutions and now being called CenturyLink Data Centers Colocation and Managed Services (DCCLMS) completes annual combined Statement on Standards for Attestation Engagements 16 (SSAE) / International Standards for Assurance Engagements 3402 (ISAE) (formerly SAS70) reports. The report covers the period October 1 through September 30 and is a Type II.
The last audit reports are available upon request with proper NDA in place. A successful completion of the SSAE 16 audit indicates that DCCLMS’ processes, procedures and controls have been formally reviewed and evaluated by an independent accounting and audit firm. This includes a review of the controls in place for managed security services, change management, service delivery, support services, backup and environmental controls, logical and physical security, managed storage, managed backup, and managed hosting (excluding virtual private data center).

DCCLMS issues a Type II combined SSAE 16 / ISAE 3402 report that covers a twelve month period. A Type II audit includes an examination of controls that have been placed in operation and testing of operating effectiveness for a period of time of at least six months. Although the findings of this audit are treated as proprietary and confidential, a copy of the SSAE 16 report is available for current customers in good standing who sign a separate SSAE 16 non-disclosure agreement (NDA). Requests can be made via your DCCLMS account team.

DCCLMS has also completed a SOC 2 Type II report. SOC 2 reports are intended to meet the needs of a broad range of users that need to understand internal control at a service organization as it relates to the Trust Service principles framework. The report is relevant to the non-financial reporting controls using the five principles of security, availability, processing integrity, confidentiality and privacy of a system.

DCCLMS’ SOC 2 program focuses on security and availability from a policy, communication, procedure, and monitoring aspect at this time for an annual time frame of October 1 through September 30. Although the findings of this audit are treated as proprietary and confidential, a copy of the SSAE 16 report is available for existing customers who sign a separate SSAE 16 non-disclosure agreement (NDA). Requests can be made via your DCCLMS account team.

9.2 PCI

DCCLMS obtained a passing Report on Compliance (ROC) for the physical security controls in certain data centers and as a separate ROC for Firewall and NIDs. While DCCLMS’ ROCs and listing on the Visa website is limited, DCCLMS does host many Level-1 and Level-2 merchants, credit card processing companies, and other parties who must demonstrate PCI compliance in environments that utilize DCCLMS’ data center facilities, network infrastructure, and managed hosting and security services. These customers have used third-party assessors (QSAs) to examine their environments hosted at DCCLMS.

9.3 HIPAA

The Health Insurance Portability and Accountability Act (“HIPAA”) is a federal statute and implementing regulations that impose standardization and protections for the interchange of electronic health and medical data (Protected Health Information or “PHI”) among health care clearinghouses, health care providers, and health plans (“Covered Entities”) in the healthcare industry. While CenturyLink as a service provider is not a Covered Entity and is not subject to HIPAA directly, we will work with customers who have to meet HIPAA requirements.
9.4 Safe Harbor/Data Protection

DCCLMS is Safe Harbor Certified in accordance with the US Department of Commerce and European Union Commission’s Directive on Data Protection guidelines. However, with the recent decision of the European Court of Justice invalidating the U.S. Safe Harbor Certification Program, CenturyLink is reviewing its options for an alternative compliance framework.

CenturyLink fully intends to retain the administrative, technical, and physical security controls currently deployed to protect customer data and support its global compliance programs as it implements other frameworks that will continue to enable data transfers across its global Hybrid IT services.

CenturyLink expects to participate in the successor program to Safe Harbor currently being negotiated by authorities. In the meantime, or if no successor program is adopted, CenturyLink will review alternative data transfer frameworks with customers, including the use of the Standard Contractual Clauses.

9.5 Service Audits

CenturyLink recognizes that customers may need to conduct an on-site audit of service delivery. In most instances, CenturyLink permits customers to conduct such audits at its own expense once each calendar year. This service audit may be performed by any third-party auditor(s) designated by the CenturyLink customer who enters into a standard CenturyLink Auditor Access and Confidentiality Agreement.

The Service Management organization will coordinate and make available all documents and records related to CenturyLink’s provision of the customer’s service(s). CenturyLink will provide customer with reasonable access to any CenturyLink facilities used to provide services for the purpose of customer’s inspection of the equipment and facilities which are used by CenturyLink to provide the service(s). Service audits and facility access must occur during CenturyLink’s normal business hours and must be scheduled at least ten business days in advance.

All auditors will be escorted by CenturyLink personnel during this period of access. CenturyLink will provide escort service at no additional charge for up to four hours for each such audit. Thereafter escort services shall be chargeable. If physical inspection is not permitted or practical, CenturyLink will review with customer and its designated auditor logical diagrams, rack elevations, and/or equipment inventory lists documenting in detail the installed Service(s). Customers cannot have access to the security operations center, managed hosting center, or another CenturyLink customer’s area at any CenturyLink facility.

10. DISCLOSURE STATEMENT

This internal CenturyLink document is provided to customers under confidentiality restrictions for informational purposes and nothing herein creates any obligation, contractual or otherwise, between the parties and no third-party beneficiaries are intended. CenturyLink makes no representations that any of the information provided herein satisfies any legal or industry data security standard. Any information provided herein by CenturyLink is made in good faith on an “AS IS” basis as to its accuracy at the time of disclosure. The corporate Information Security policy addresses non-compliance with a policy or process and CenturyLink disclaims any responsibility or liability regarding the same.