Physical Security

Administration Standards

for Suppliers

September 2020

Version	Date Published	Business Process Owner (Region)	Document Writer	Summary Of Changes
1.0	9/11/2020	Jeff Hay	Brandon Gipson	First Release

1 Overview

1.1 Purpose

CenturyLink expects all agents, consultants, contractors, subcontractors, suppliers and other business partners (collectively "Suppliers"), as well as their respective employees, agents, contractors, subcontractors, and representatives ("Supplier Personnel") with whom CenturyLink does business to embrace and share CenturyLink's commitment to security and compliance with the law.

As part of CenturyLink's ongoing effort to protect its information, equipment and personnel, CenturyLink requires all Suppliers to adhere to certain physical security standards while doing business with CenturyLink. This document sets forth the minimum physical security standards required by CenturyLink of its Suppliers.

Particular Supplier contracts may contain security standards or provisions that are more specific than the standards set forth in this document. Nothing in this document is meant to supersede any more specific contractual provision. To the extent any provision of this document is inconsistent with any applicable contractual provision, the contractual provision will control to the extent not inconsistent with applicable law.

1.2 Exception to Standards

Exceptions to these Standards are not permitted unless approved in writing by CenturyLink Physical Security. Exception requests may be sent to: RegionalSecurityReps@Lumen.com

2 Documentation

2.1 General

Suppliers are expected to maintain written documentation incorporating these minimum physical security standards into Supplier security programs or procedures. This written documentation must be made available to CenturyLink Physical Security upon request.

3 Security Reporting

3.1 Security Incident Reports

All security incidents that impact or may impact the security of CenturyLink information, equipment, or personnel must be documented and immediately reported to CenturyLink UNIcall at 866-864-2255, option 4. Examples of incidents to be reported include:

- physical assault or threats of violence
- bomb threats
- burglary, robbery, or theft
- missing or damaged property
- computer hacking
- Physical or information security breaches
- embezzlement, kickbacks, misuse of funds, or other fraud
- misconduct by employees, vendors or contractors
- misappropriation or misuse of CenturyLink property or information

The above examples are illustrative. Supplier is expected to exercise good judgment in assessing whether a particular incident does or may impact CenturyLink information, equipment or personnel. In the event of uncertainty, the event should be reported.

4 Responsibilities When Working in CenturyLink Facilities and Premises

4.1 General

Suppliers working in CenturyLink facilities have the following security-related responsibilities:

- protect and safeguard all CenturyLink property, personnel, and information within their control;
- ensure all doors and other entry points are appropriately locked and secured;
- report malfunctioning locks, doors and other security devices;
- report known or suspected physical or information security breaches;
- report known or suspected damage, destruction, misappropriation or misuse of CenturyLink property or information;
- ensure all individuals under Suppliers control, including visitors, comply with security rules, policies and procedures and do not pose a risk to people, property or information;
- comply with all postings or notices located on CenturyLink premises regarding safety, security, and weapons; and,
- Immediately report all known, perceived or suspected security concerns.

4.2 Supplier Personnel Responsibilities

Suppliers are responsible for ensuring Supplier Personnel who are given or obtain access to CenturyLink premises or facilities comply with these security standards and require the same level of compliance of their own employees, contractors, vendors, agents and partners.

As part of their security-related responsibilities, Supplier and Supplier Personnel shall ***not***:

- carry weapons or ammunition onto CenturyLink premises or use or carry weapons while performing services or attending CenturyLink-sponsored activities;
- attempt to circumvent security rules, policies and procedures;
- attempt to circumvent, disable, or defeat locks or other security devices or systems;
- attempt to enter facilities or areas of facilities they are not authorized to enter;
- loan or share access/identification badges, access codes, keys, combinations or other access devices/methods assigned to them;
- use their access/identification badges, access codes, keys and other access devices/methods assigned to them to grant facility or area access to unauthorized individuals; or
- otherwise permit unauthorized personnel to enter facilities or restricted areas of facilities.

5 Access Control

5.1 General

Suppliers must establish access control processes and procedures that apply to all Supplier facilities containing CenturyLink information, personnel and equipment. These processes and procedures must minimally meet the security standards for access controls set forth in this document and must be sufficiently tailored to protect against unauthorized access to CenturyLink information, personnel, and equipment.

5.2 Access Cards/ Identification Badges

Where Suppliers use access cards and/or identification badges to control access to their facilities, the following is required:

- Suppliers must only provide access cards and/or identification badges to individuals who are authorized and have a frequent and recurring need to access areas containing CenturyLink information, personnel and/or equipment;
- Suppliers must retrieve access cards and identification badges on a timely basis when it is determined that access is no longer required by the individuals to whom this access was issued;
- Suppliers must revoke or reprogram access when individuals to whom access was granted no longer authorized;
- Suppliers must review and validate access lists for areas containing CenturyLink information, personnel and/or equipment at least quarterly to ensure individuals on those lists should continue to be authorized; and
- the loss or theft of access cards/identification badges must be reported and acted upon immediately.

5.3 Lost or Forgotten Access/ Identification Cards

Where Suppliers use access cards and/or identification badges to control access to its facilities, Suppliers must establish appropriate procedures to ensure that Supplier Personnel or other individuals who claim they have lost or forgotten issued access/ identification cards are authorized prior to granting access. The procedures must include:

- verifying authorization of Supplier Personnel (a) by contacting the employee's supervisor or Human Resources; or, (b) for non-employees, by contacting an appropriate management official or authorized representative; and,
- verifying identity through either government-issued photo identification or visual recognition.

If temporary access cards are issued, Suppliers must implement a process to document the card's issuance and to retrieve and/or deactivate the temporary card promptly when it is no longer required to provide services to CenturyLink.

6 Visitor Processing and Control

6.1 General

Visitors are individuals who have not been granted specific, unescorted access privileges to a particular area or facility via an access device (e.g. access card, identification badge, key, lock code or combination). All Supplier Personnel without unescorted access privileges to a particular area or facility must be treated as a visitor if the area or facility to which they require access contains CenturyLink information, personnel or equipment.

Suppliers must establish and implement the following minimum-security procedures for the documentation and control of visitors to Supplier facilities or areas containing CenturyLink information, personnel, or equipment:

- verify the identity of all visitors through government-issued photo identification (e.g., driver license, passport, etc.) or a supplier-issued photo identification badge;
- maintain a record of all visitors inclusive of the visitor's full name, organization, date and time of arrival, date and time of departure, and individual(s) visited;
- visitors must wear a distinctive and highly visible "visitor badge" while in the facility; and
- visitors must be escorted at all times while in areas containing CenturyLink information, personnel or equipment.
- visitor registration documentation and records must be retained for a period of one (1) year and provided to CenturyLink for review upon request.

7 Access Devices

7.1 Usage

Supplier Personnel may be issued an access device (e.g., access card, identification badge, key, lock code, etc.) authorizing access to certain CenturyLink facilities.

Identification badges/ access cards **must be visibly worn** by Supplier Personnel at all times while on CenturyLink property. Any incident resulting in the loss or compromise of the access device must be immediately reported to the CenturyLink sponsor of the individual to whom the device was issued.

Supplier Personnel **are not permitted** to:

- loan an access device to another person;
- use an access device to grant access to another person or people;
- enter CenturyLink premises, except during authorized hours and in conjunction with their CenturyLink-related duties;
- enter CenturyLink premises to solicit business or to develop contacts to solicit business in the future; or
- engage in any other activity that would constitute abuse of their access privileges.

8 Lock and Key Programs

8.1 General

If building locks are used to protect CenturyLink information, personnel and/or equipment, Suppliers must establish an effective lock and key program that complies with this section.

8.3 Spare Equipment Storage

Suppliers must establish an appropriate level of protection over spare keys, key blanks, key manufacturing equipment, key records, etc. to ensure access only by authorized individuals.

8.4 Employee Awareness

Supplier Personnel must be trained on their duties and obligations relative to the safeguarding of keys issued to them. These include, but are not limited to, never loaning keys to others, never duplicating keys, immediately reporting lost or stolen keys, and returning keys upon request or when they are no longer needed for assigned

duties.

8.5 Lost or Stolen Keys

Suppliers must conduct risk assessments for all lost or stolen keys. When a risk assessment indicates the lost or stolen key creates vulnerability, Suppliers must take appropriate steps to mitigate the vulnerability as it pertains to CenturyLink information, personnel and/or equipment.

8.6 Pushbutton Locks

CenturyLink, at its discretion, shall prohibit the use of push-button-type locks for the protection of some areas containing CenturyLink information, personnel and/or equipment. Where push-button type locks are employed, Supplier must ensure:

- codes are distributed only to authorized individuals;
- individuals to whom the codes are issued understand they must safeguard them and not provide them to others;
- codes are changed no less frequently than on a quarterly basis; and
- codes are changed immediately if there is reason to believe the code has been compromised or where prior authorization to any individual has been revoked or is no longer needed.

9 Intrusion Detection Systems

9.1 General

Where Suppliers employ intrusion detection systems to protect CenturyLink information, personnel and/or equipment:

- alarm signals must terminate in a monitoring location that is staffed 24x7;
- the alarm system or individual sensors shall not be masked;
- defined response procedures must be established and implemented for all alarm types; and,
- there must be a human response to all alarms for alarm analysis purposes.

Please note that CenturyLink may require the use of intrusion alarms in certain situations.

10 Photography and Tours

10.1 General

Image recording within areas containing CenturyLink information, personnel and/or equipment, and tours of such areas, are not permitted without the written authorization by CenturyLink Physical Security. This applies to all image-capturing devices with either traditional or digital imaging capabilities. This includes all cellular phones, tablets and electronic devices with digital imaging capabilities, cameras, camcorders, etc.

11 Physical Security Assessments

11.1 General

It is the responsibility of CenturyLink Corporate Security to conduct physical security assessments of facilities housing CenturyLink information, equipment, personnel and/or operations for the purpose of identifying risks to CenturyLink. Suppliers will cooperate with those assessments by providing timely access to pertinent facilities, areas, personnel, systems, equipment and documentation.