Physical Security Administration

Standards for Suppliers

Table of Contents

1 Overview

1.1 Purpose

To provide an appropriate level of protection for CenturyLink information, equipment and personnel, certain physical security requirements must be met in the day-to-day administration of supplier security programs.

The purpose of this document is to set forth minimum physical security requirements CenturyLink suppliers are expected to maintain or observe to provide an appropriate level of protection for CenturyLink information, equipment and/or personnel.

1.2 Exception to Standards

Exceptions to any item listed in this standard must be requested from, and approved by, Corporate Security. Exceptions to these standards can be requested by submitting the request in writing to the Corporate Security department.

2 Documentation

2.1 General

Suppliers must formally document supplier programs, methods, processes and/or procedures designed to meet the requirements of this document and will make the documentation available for review by CenturyLink Corporate Security personnel upon request.

3 Security Reporting

3.1 Security Incident Reports

Security incidents that impact, have the potential to impact, or suggest a possible future risk to CenturyLink information, equipment or personnel must be documented and reported to CenturyLink UNIcall 866-864-2255, option 4. Examples of the types of incidents to be reported are:

- Assault
- Bomb Threat
- Burglary
- Computer Hacking
- Embezzlement
- Fraud
- Misconduct by Employees, Vendors or Contractors
- Property Damage
- Robbery
- Suspicious Activities, People or Situations
- Missing Property or Theft
- Threats

These examples are not intended to constitute an exhaustive listing. Supplier is expected to apply appropriate judgment and recognize and report other incidents that impact, or may impact, CenturyLink information, equipment or personnel.

4 Responsibilities When Working in CenturyLink Facilities

4.1 General

Suppliers working in CenturyLink facilities have certain security-related responsibilities. They are required to:

- Protect and safeguard the CenturyLink property, personnel and information in their control;
- Ensure doors and other entry points they use close and lock properly;
- Report malfunctioning locks, doors and other security devices;
- Report suspected or known breaches of security;
- Report suspected or known damage, destruction, misappropriation or misuse of CenturyLink property, or information;
- Ensure their visitors, or other individuals under their control, comply with security rules, policies and procedures, and do not pose a risk to people, property or information; and
- Comply with all postings or notices located at CenturyLink premises regarding safety, security or weapons.

4.2 Supplier Personnel Responsibilities

Suppliers must ensure their employees working at CenturyLink facilities comply with these requirements, and must implement these same requirements for their employees, contractors and vendors at any facility housing CenturyLink information, equipment and/or personnel. As part of their security-related responsibilities, supplier employees, contractors and vendors working in CenturyLink facilities, shall ***not***:

- Carry weapons or ammunition onto CenturyLink premises or use or carry weapons while performing services or attending CenturyLink-sponsored activities.
- A clear desk policy must be enforced. Documents that contain CenturyLink Data must be kept secured (e.g. locked office or file cabinet) when not in use.
- 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 and 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.

Suppliers must ensure their employees working at CenturyLink facilities comply with these requirements, and must implement these same requirements for their employees, contractors and vendors at any facility housing CenturyLink information, equipment and/or personnel.

5 Access Control

5.1 General

Suppliers must establish access control processes and procedures for all supplier facilities containing CenturyLink information, personnel and/or equipment. Suppliers' processes and procedures must provide CenturyLink an appropriate level of assurance that only authorized personnel have access to CenturyLink information and/or equipment and, at a minimum, must meet the requirements for access control that are set forth in this document.

Physically secure perimeters and external entry points must be suitably protected against unauthorized access (e.g. barriers such as walls, card controlled entry gates). Access to all locations must be limited to Supplier Personnel and authorized visitors only. Reception areas must be manned or have other means to control physical access.

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 they are no longer required by the individuals to whom they were issued;
- Suppliers must reprogram accesses when the individuals to whom they were issued are no longer authorized to access areas containing CenturyLink information, personnel and/or equipment;
- 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 individuals who claim they have lost or forgotten issued access/identification cards are authorized prior to granting access. The procedures must include verifying:

- Employment status of employees through their supervisor or Human Resources;
- The status of non-employees through contact with an appropriate management official; and
- 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 the individual using it no longer needs it to provide services to CenturyLink.

6 Visitor Processing and Control

6.1 General

Visitors are individuals who have not been granted unescorted access privileges through a key, code, combination or an access card programmed to provide access to the facility/area in question. Supplier employees not assigned to a facility or area shall, therefore, be treated as visitors for that facility or area. Suppliers must establish the following procedures for the documentation and control of visitors to supplier facilities containing CenturyLink information, personnel and/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, to include full name, organization, date/time of arrival, date/time of departure, and individual visited;
- Have the visitor wear a distinctive and highly visible "visitor badge" while in the facility; and
- Escort visitors at all times while in areas containing CenturyLink information, personnel and/or equipment.
- Suppliers must retain visitor registration documentation and records for a period of one (1) year and provide it to CenturyLink for review upon request.

7 Access Devices

7.1 Usage

If supplier personnel are issued access devices (e.g., access cards, identification badges, keys, lock codes, etc.) for CenturyLink facilities, supplier personnel are required to:

- Wear identification badges/access cards in a visible manner at all times while on CenturyLink property;
- Immediately report the loss or compromise of an access device to the regional physical security representative for your area as identified through the following link. https://qtdenvmpc044/psweb/contact_cacc.htm
- Return the access devices when no longer needed, or upon request.

If supplier personnel are issued access devices (e.g., access cards, identification badges, keys, lock codes, etc.) for CenturyLink facilities, supplier personnel **are not permitted** to:

- Loan the devices to other people;
- Use the devices to grant access to other people;
- Enter company facilities, or areas of facilities, except in conjunction with their CenturyLink-related duties;
- Enter company facilities, or areas of facilities, for the purpose of solicitation of business or for the purpose of developing contacts with the intent of solicitation of business at a future date; or
- Engage in any other activities 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 must that complies with this section.

8.2 Key Records

Suppliers' key records must document the following:

a) Key identifier code;
b) Date of issue;
c) Date of return;
d) Name of the individual to whom the key was issued;
e) Type of key (control, master, operating, etc.); and
f) Status of the key (i.e., issued, lost, returned, destroyed, or held in inventory).

8.3 Spare Equipment Storage

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

8.4 Employee Awareness

Suppliers must make its employees aware of the requirement to safeguard keys issued to them, the fact that keys shall not be loaned to others, that they must immediately report lost or stolen keys, and that keys must be returned upon request or when 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 shall not provide them to others;
- Codes are changed on a quarterly basis; and
- Codes are changed immediately if there is suspicion the code has been compromised or an individual to whom the code was issued is no longer authorized access to the area protected by the lock.

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 for all alarm types; and
- There must be a human response to all alarms for alarm analysis purposes.
- CenturyLink may require the use of intrusion alarms in certain situations.

10 Photography and Tours

10.1 General

Photography within areas containing CenturyLink information, personnel and/or equipment, and tours of such areas, are not permitted without the written permission of a CenturyLink regional physical security representative for your area/region as identified through the following link.
https://qtdenvmpc044/psweb/contact_cacc.htm

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.

Revision History

Date	Description
May 2006	Standards published.
September 2006	Reviewed; no major revisions made.
March 2007	Reviewed; no major revisions made.
October 2007	Updated wording in various sections of the document. Added the following new sections: • 2 – Documentation • 4.1 – Responsibilities When Working in CenturyLink Facilities; General
February 2009	Reviewed; no major revisions made.
November 2009	Reviewed; no major revisions made.
December 200+	Reviewed and Updated Added 1.3 Exceptions to Standards
September 2011	Reviewed and updated Updated 1.2 Updated 3.1 Updated 7.1 Updated 10.1
March 2016	Updated Web Links and contact information Updated 4.2 Updated 5.1