



CenturyLink Disaster Preparedness

□ Overview

Contents □

- Overview & Governance
- Best Practices & Staffing
- Planning Approach
- Key Plan Elements
- BC Plan Table of Contents
- Crisis Management
- Sustainability

CenturyLink has a comprehensive Business Continuity Management (BCM) program that supports all of its organizations throughout our global operations.

The BCM program is designed to ensure that CenturyLink is prepared to continue providing services to our customers in the event of a significant business disruption.

CenturyLink's commitment to the BCM program is reflected in its institution of corporate standards regarding plan development, personnel involvement, as well as, plan reviews and updates.

This document summarizes CenturyLink's business continuity management program and related disaster preparedness activities.



“Improving the lives of our customers by connecting them to the power of the digital world.”

CenturyLink's Objectives

During the 2013 Colorado floods, two CenturyLink helicopters rescued roughly 16 people, and 10 cats and dogs, near the mountain town of Drake.

Policy □

- Annual organizational review to denote changes in key personnel or processes
- Annual training for key personnel
- Key process plans reviewed exercised periodically

□ Governance

Corporate Policy.

CenturyLink's corporate policy requires its organizations to develop business continuity plans, disaster recovery plans, and crisis communication strategies.

Plans are to be maintained for critical functions and technology that, if disrupted, would significantly impact our ability to provide customer services.

Leadership Involvement.

CenturyLink leaders support the Disaster Preparedness programs by assigning program partners to represent their organization's interest in operational resilience.

Recognized Standards.

In addition to a number of planning elements required by regulation, we have aligned our program to adhere to



CenturyLink Disaster Preparedness

ISO22301 standards.



CenturyLink Disaster Preparedness

Best Practices



Replacing a pedestal from the 2014 Washington State wildfire.

CenturyLink’s program and plans have been developed with the involvement of certified business continuity professionals (MBCP, CBCP, and MBCI), who incorporate best practices acknowledged by Disaster Recovery Institute International (DRII) and the Business Continuity Institute (BCI). Best practices employed by CenturyLink include, but are not limited to:

- Threat Assessment & Business Impact Analysis results as a basis for Business Continuity planning
- Geographic diversity of recovery resources
- Consideration of third-party resources
- Multiple business resumption options for critical functions
- Routine plan reviews, updating and testing
- Consistent and integrated planning approach across the enterprise

Disaster Preparedness Staffing

Team	Roles & Responsibilities – All Levels
Leadership	CenturyLink leaders are responsible for providing direction following an event that may have consequences beyond those typically managed by the corresponding Event Management team.
Regional Event Management	Four regional teams are led by regional operations directors and comprised of representation from all critical business and support units at the local level. These teams are activated when there is an event that affects, or has the potential to affect, one or more business units or key functions in a geographic area.
Disaster Preparedness	CenturyLink staffs a full-time group of disaster preparedness professionals to oversee and support all elements of the corporate program. Staff members hold CBCP and MBCI certifications, graduate degrees, and have experience in telecommunications or IT operations. Supported elements include: Business Continuity Management, Disaster Recovery, Workforce Contingency Planning, Crisis Response and Communications Management.



CenturyLink Disaster Preparedness

Crisis Communications

CenturyLink's business units are represented within this structure and activated whenever there is a severe, multi-region business interruption or potential threat to the corporation at large. Primary and alternate team members provide corporate-wide resources to assist regional teams in addressing key issues, identifying support needs, and coordinating recovery activities within their respective business units. Team members participate in drills, crisis simulations, and receive annual training.



CenturyLink Disaster Preparedness

Team	Roles & Responsibilities – All Levels
Business Continuity Managers & Planners	Disaster Preparedness resources within each organization, and subsequent business unit, are responsible for assisting in the identification of key business processes and their resource recovery needs. These individuals engage subject matter experts to validate the developed plans through the review and exercise process.
IT Disaster Recovery Services	This group is responsible for all application and hardware recovery plans, as well as integrating outage management with Disaster Preparedness’s crisis communications activities. This group coordinates the IT Incident Management Team, which is a “SWAT-like” team designed to manage rapid application recovery.
Damage Assessment & Rapid Response	These teams include individuals familiar with network elements, engineering and construction processes who mobilize on short notice. People used in this effort have hands-on experience or working knowledge of the network infrastructure and may include engineers, technicians or other subject matter experts with the training and skills to make accurate preliminary reports.
Network Reliability Operations Center	The Network Reliability Operations Center (NROC) organization staffs a 24x7x365 center that monitors our telecommunications network to rapidly identify potential issues and respond to real-time outages. The NROC is the focal point for network restoration, and is an integral component of the overall crisis management structure.
Environmental Health & Safety	CenturyLink is committed to protecting the environment and the health and safety of our employees, customers and the communities we serve by conducting our business in a safe and environmentally responsible manner. The Environmental Health and Safety staff provides support to the business units and is engaged at all levels during major events or disasters.



CenturyLink Disaster Preparedness

□ Planning Approach



In order to avoid disruptions to services, you need to have a plan. We have a plan. In fact, we have several plans that are designed to minimize disruption of

CenturyLink services. The plans address critical internal business functions that, if disrupted, could lead to service outages.

Approach	Planning Description
Enterprise-Wide Scope	<p>CenturyLink recognizes that large enterprises continually increase in complexity and interdependence, and that no functions operate in isolation. Accordingly, CenturyLink’s business continuity plans address critical functions concerning the recoverability of CenturyLink’s technological infrastructure, the ability to provide customer support to new and existing customers, and the ability to receive and fulfill customer orders. Each of these plans recognizes and accounts for operational interdependencies involving both internal and external resources. CenturyLink’s plans engage company resources from around the globe for the purposes of continuing critical business functions.</p>
All-Hazards Planning	<p>CenturyLink’s all-hazards approach to business continuity planning focuses on the impacts that may result from a broad range of natural disasters, infrastructure failures, and human-induced disasters. Consequently, 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.</p>



CenturyLink Disaster Preparedness

Strategic Diversity

CenturyLink employs the use of multiple business continuity strategies in business continuity plans. By using a combination of mutual support agreements, remote work arrangements, technology failover and redundancy and third-party agreements, we believe that our plans enable us to effectively respond to business disruptions. This approach allows us to respond, even in light of the uncertain and the dynamic nature of current and potential threats.



CenturyLink Disaster Preparedness

Approach	Planning Description
Compliance Management	<p>The CenturyLink Compliance Management team is dedicated to continually improving and maintaining compliance certifications that are critical to our customers. Through our disciplined assessment and audit processes, CenturyLink has implemented comprehensive practices for SSAE 16 SOC 1, SOC 2, PCIDSS, ISO 27001, Safe Harbor, Global Risk Management, Business Continuity and Disaster Recovery (BCDR), HIPAA, and FISMA (NIST 800-53). We engage external audit firms to perform multiple types of assessments designed to address our customers' diverse compliance requirements.</p>
Public Health Risks/Staffing/Absenteeism	<p>CenturyLink has incorporated into its business continuity planning a methodology to address potential or significant disruptions in employee staffing levels. A Health Risk Assessment and Strategic Response plan has been implemented to establish a framework which potential health risks (contagious and non-contagious) can be identified, assessed, monitored and acted upon if necessary. The plan provides a system of on-going and proactive situational awareness to identify potential health risks to the organization; creates an internal Strategic Health Risk Management Team to assess impacts to the organization and establish and implement plans and protocols to mitigate the impact of the risk on CenturyLink; establishes general health maintenance procedures to be implemented throughout the organization to prepare for and minimize routine health risks; and develops threat specific guidelines to assist in understanding preparation and response to health risks. Additionally, CenturyLink maintains a comprehensive wellness program that includes influenza vaccinations at no-charge.</p>
Dedicated Resources	<p>CenturyLink has dedicated business continuity resources on a full-time and a part-time basis. Full-time disaster preparedness managers act as internal consultants to business units to identify and help implement planning needs. Subject matter experts and leaders within each business unit provide detailed technical expertise to support the development and maintenance of preparedness activities.</p>
Training & Awareness	<p>Strategic CenturyLink employees participate in quarterly disaster awareness meetings, business continuity training, and receive targeted emails.</p>



CenturyLink Disaster Preparedness

Exercise Resources

CenturyLink performs annual testing through checklist, tabletop, simulation exercise or actual events. Any gaps are identified, documented and tracked to resolution.



CenturyLink Disaster Preparedness

Key Plan Elements

While specific business continuity plan contents are proprietary, CenturyLink is pleased to summarize plan contents for its current and future customers, and for its insurers.

CenturyLink uses a standard planning model across the enterprise to facilitate consistency in planning and to optimize integration of departmental plans. Major plan elements include:

Approach	Planning Description
Immediate Actions	As business disruptions frequently accompany emergency situations, CenturyLink plans describe how employees transition from an emergency situation to business resumption activities, whether they are at the office or away from work.
Internal Communications	CenturyLink plans describe internal communications that are required to engage company resources in order to implement business continuity measures and to inform appropriate CenturyLink departments and employees that may be impacted by the event.
Business Resumption Procedures	CenturyLink plans provide department-specific, step-by-step instructions and/or options that will be implemented to resume critical functions if a CenturyLink site is inaccessible or if essential resources are unavailable. Procedures may involve transition of work to alternate locations, re-prioritization of work activities, establishing virtual offices, implementing manual contingencies, and others.
External Communications	CenturyLink plans describe how the company will communicate with customers, suppliers, contractors, business partners, media and other entities that may be impacted by a disruption or are vital to continuing critical business functions. CenturyLink is a member of the National Communications System to ensure telecommunications are available and prioritized through the Government Emergency Telecommunications Service and Wireless Priority Service.



CenturyLink Disaster Preparedness

Vital Resources

CenturyLink plans describe how departments obtain resources that are necessary to perform critical functions. Resources may include vital records and data, computing equipment, human resources, and others.



CenturyLink Disaster Preparedness

Approach	Planning Description
Disaster Service Support	CenturyLink retains support for disaster services in the areas of cloud services, facility recovery, records recovery, and telecommunications recovery. These services assist CenturyLink by providing technical telecommunications support related to network element protection, response and recovery recommendations.
Mutual Aid	CenturyLink has agreements with major telecommunication companies to provide mutual support in the event of a disaster. CenturyLink has both provided and received support as a result of the mutual aid agreement. Examples of when support was both given and received include a recent flood and hurricane.
Disaster Recovery Trailers	CenturyLink owns seven mobile switching trailers that can be rapidly deployed to assist in the recovery of a damaged switch location. Trailers are geographically dispersed for nationwide deployment and operate on both commercial power and an on-board diesel generator.

BC Plan Table of Contents

Business Continuity Plans.

This is an outline of the plan contents and it describes the actions to be taken in the event that critical business functions are disrupted.

SECTION 0: BUSINESS CONTINUITY PLAYBOOK

- 0.0 Online Copy Requirements
- 0.1 Hardcopy Copy Requirements

SECTION 1: IMMEDIATE ACTIONS

- 1.0 If at the Workplace
- 1.1 Secondary Assembly Locations
- 1.2 If Away from the Workplace

SECTION 2: BUSINESS CONTINUITY PROCEDURES

- 2.1 Critical Functions
- 2.2 Location Contingencies - Alternate Work Arrangements
- 2.3 Technology Disruption Contingencies
- 2.4 Staffing Contingencies
- 2.5 Other

SECTION 3: INTERNAL COMMUNICATIONS

- 3.1 Crisis Communications
- 3.2 Department Leadership
- 3.3 Department Key Personnel
- 3.4 Crisis Management Team Representative

SECTION 4: EXTERNAL COMMUNICATIONS

- 4.1 Vendors/Suppliers
- 4.2 Customers
- 4.3 Regulators

APPENDIX 1: VERSION CONTROL

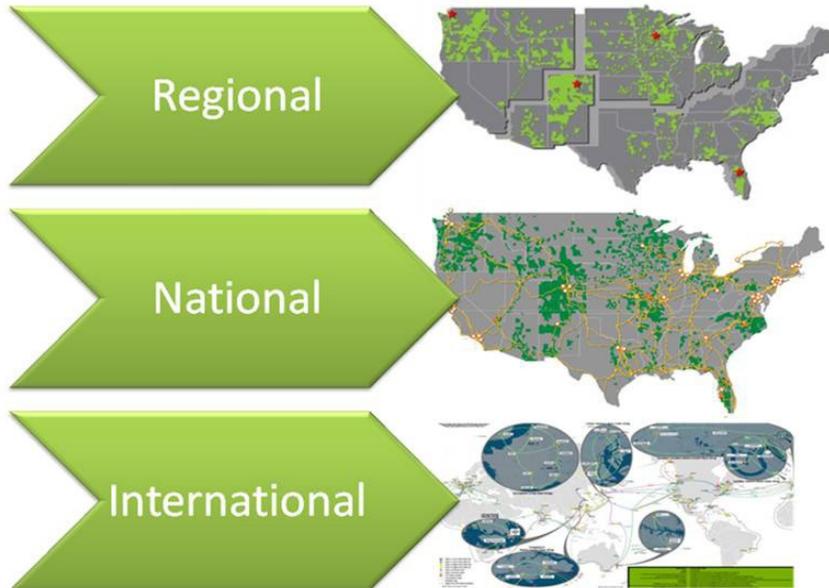
APPENDIX 2: PLAN STRUCTURE & CONTENT

- A1.10 Security and Handling Instructions
- A1.20 Purpose and Scope



□ Crisis Management Structure

Crisis Management Structure



Crisis Management Structure.

While we are proud of our continuity planning, we also know that disasters happen, and we must be ready to respond to them quickly.

Crisis Management Framework.

CenturyLink has developed a three-layer crisis management approach. Regional, National and International Command Centers involve key leaders, decision-makers, and subject matter experts at all levels of the organization.

The system is similar to the Incident Command System used by federal response agencies, but is tailored to meet the needs of CenturyLink.

Team members participate in an annual exercise, as well as more frequent activation drills.

□ Command Centers



The corporate Command Center is located in Littleton, Colorado. It is equipped with multiple media sources, telecommunications diversity, HF radio, emergency power, robust computer support, and various emergency supplies.

CenturyLink also maintains regional Command Centers that are equipped with, at a minimum, emergency power, and robust IT and telecommunications.



CenturyLink Disaster Preparedness

□ Crisis Management Support



CenturyLink has established contractual relationships with several disaster services companies to assist in recovery operations.

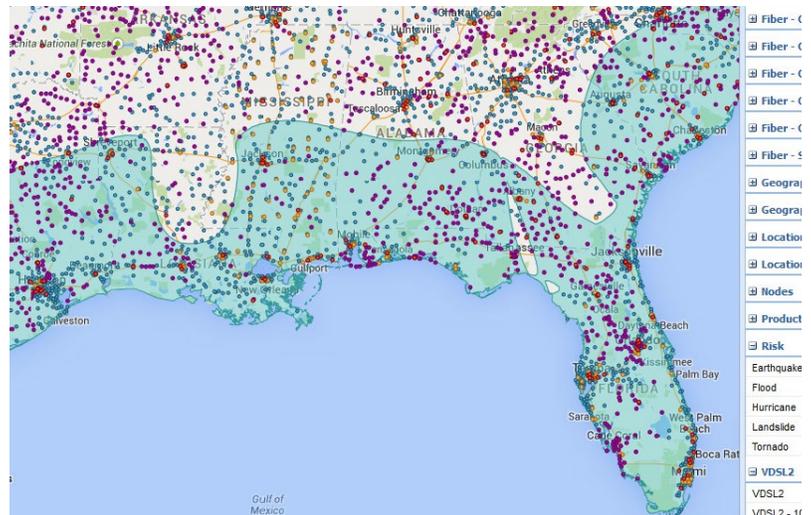
These service companies are available to provide 24x7x365 support nationwide.

CenturyLink maintains contracts that provide telecommunications-specific support.

□ Geographic Information Systems

We believe that our risk assessment decision support is greatly enhanced by the use of Geographic Information Systems (GIS). This enables CenturyLink to rapidly acquire situational awareness during an event, thus improving decision-making and reducing the time required to make those decisions.

CenturyLink continuously expands its use of GIS by building or updating additional layers of information gained during a business impact analysis and site threat assessments. CenturyLink gets automated alerts based on the proximity of incidents to more than 70,000 sites that we monitor for a fast response.

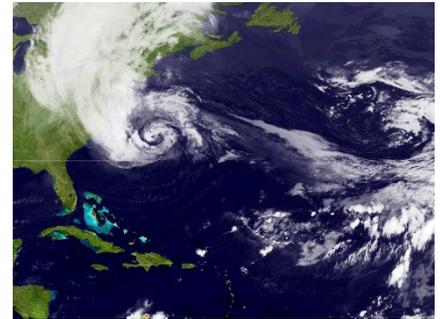




CenturyLink Disaster Preparedness

Environmental Sustainability

Super Storm Sandy drew attention to the increasing climate-related risks for communities and businesses. Weather related disasters are happening more frequently and with greater intensity. CenturyLink supports greening initiatives that aid the environment while aligning with recovery objectives. That is why the CenturyLink Environmental Sustainability Governance Council, the “Green Team,” was created. CenturyLink’s risk-based approach to disaster mitigation focuses on the hydrological cycle, biodiversity, slope, topography, water quality, and climate.



Storm hardening requirements are considered in the engineering and design process. This elevated cabinet, positioned on coastal terrain, was built 20 feet in the air to avoid storm surge.



Alternative Energy. CenturyLink is expanding its sustainability commitments by installing Bloom Energy fuel cells to generate up to 500 kilowatts of clean power for one of its Irvine, California data centers. This configuration enables CenturyLink to receive primary power for its critical loads from Bloom Energy Servers, protecting those loads from electrical outages without the need for backup UPS and generator systems.

Environmentally Sound Disaster Strategy. Although our industry faces many environmental challenges, CenturyLink is committed to working toward solving them. CenturyLink uses remote work strategies to minimize the impact to customers and the environment during disasters. Environmentally sound data center design and virtualization contribute to resiliency, high availability, and recoverability.

Contact Us

For more information, please contact CenturyLink Disaster Preparedness:
DPER@CenturyLink.com