



# 2013 CenturyLink Disaster Preparedness White Paper

## Business Continuity Program Overview

### Contents

Disaster Preparedness Governance .....	2
Disaster Preparedness Best Practices .....	3
Business Continuity Planning.....	5
Crisis Management .....	8
Disaster Preparedness Sustainability .....	10

**Overview.** CenturyLink has a comprehensive incident management structure and business continuity plans for critical functions occurring throughout the enterprise, and at locations across the U.S. and internationally. We designed these plans 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 business continuity planning is reflected in its institution of corporate standards regarding plan development, review, training, updating, and testing. This document summarizes CenturyLink’s crisis management and business continuity program, plans, and related activities.

“Assure the continuation of CenturyLink’s mission critical business operations and services with the goal to minimize financial impacts and damage to the CenturyLink brand, its employees and customers following significant business disruptions.”

– Disaster Preparedness Mission Statement



# Disaster Preparedness Governance

## Enterprise Support and Commitment

**Corporate Policy.** CenturyLink's corporate policy requires the development of business continuity plans, disaster recovery plans, and crisis management capabilities. Plans are to be developed for critical functions and technology that, if disrupted, would significantly impact our ability to provide customer services. Each year, CenturyLink executives acknowledge that appropriate plans have been developed and provide direction regarding the development of new plans.

CenturyLink has also established the following minimum business continuity and disaster recovery standards:

- **Key individuals named in plans will be trained annually**
- **All plans will be tested or reviewed annually**

**Executive Involvement.** CenturyLink executives support the disaster preparedness programs in two ways:

1. they are an integral part of crisis management and form the Executive Crisis Team, and
2. they receive periodic briefings on the state of CenturyLink preparedness and acknowledge plans have been developed. CenturyLink business unit leaders are briefed annually on preparedness goals and objectives at the beginning of each year, and as warranted by changes in company operations.

**Recognized Standards.** In addition to a number of planning elements required by regulation, we have aligned our program with the NFPA 1600 Standard on Disaster/Emergency Management and Business Continuity Planning. CenturyLink is in the process of adopting the ISO22301 Standards and expects them to be integrated by 2015. The Crisis Management Team has adopted TL9000 and expects to be certified in 2013. These standards are reflected in Business Continuity, Disaster Recovery, and Crisis Management activities.



# Disaster Preparedness Best Practices

## Program, Plans, and People

**Certified.** CenturyLink’s program and plans have been developed with the involvement of certified business continuity professionals (MBCP, CBCP, and MBCI), and 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:

- Using Threat Assessment & Business Impact Analysis results as a basis for BC 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.** CenturyLink has established teams to respond to any incident.

Team	Roles & Responsibilities – Key Individuals Involved at All Levels
<b>Executive</b>	CenturyLink executives are responsible for providing c-suite leadership and direction following a catastrophic event, or an event that may have consequences beyond those typically managed by the Crisis Management Team.
<b>Disaster Preparedness</b>	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.
<b>Regional</b>	Five regional CenturyLink teams are led by a regional director and comprised of representation from all critical business and support units at the local level. These teams are activated whenever there is an event that affects or has the potential to affect one or more business units or critical business functions in a geographic area. In addition, these teams provide assessment and recommendations to the Crisis Management Team when that team has been activated.



# Disaster Preparedness Staffing Program, Plans and People



Team	Roles & Responsibilities – Key Individuals Involved at All Levels
<b>Crisis Management</b>	<p>CenturyLink’s critical 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 as necessary 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.</p>
<b>Business Continuity Leaders and Planners</b>	<p>Departmental business continuity leaders and planners within each business unit are responsible for assisting in the identification of critical functions and resource recovery needs. These individuals engage subject matter experts in BC planning, testing, and reviews to ensure that plans are accurate and valid.</p>
<b>IT Disaster Recovery Services</b>	<p>This group is responsible for all application and hardware recovery plans, as well as integrating outage management with Crisis Management and Business Continuity activities. This group coordinates the IT Recovery Management Team, which is a “SWAT-like” team designed to manage rapid application recovery.</p>
<b>Damage Assessment &amp; Rapid Response</b>	<p>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.</p>
<b>Network Operations Center</b>	<p>CenturyLink’s Network Operations organization staffs a 24x7x365 center that monitors our telecommunications network to rapidly identify potential issues and respond to real-time outages. The Network Operations Center is the focal point for network restoration, and is an integral component of the overall Crisis Management structure.</p>
<b>Environmental Health &amp; Safety</b>	<p>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 any major events or disasters.</p>



# Business Continuity Planning

## An All-Hazards Approach to Maximize Recoverability

**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 the opportunity for disruption to CenturyLink services. The plans address critical internal business functions that, if disrupted, could lead to service outages.

Approach	Planning Description
<b>Enterprise-Wide Scope</b>	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.
<b>All-Hazards Planning</b>	We believe that developing business continuity plans that are specific to each and every potential threat is both impractical and ill-advised, particularly with respect to a company having facilities across the globe. 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.
<b>Strategic Diversity</b>	CenturyLink employs the use of multiple business continuity strategies in all 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.
<b>Dedicated Resources</b>	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.



# Business Continuity Planning

## An All-Hazards Approach to Maximize Recoverability



Approach	Planning Description
<b>Training &amp; Awareness</b>	Strategic CenturyLink employees participate in quarterly disaster awareness meetings, business continuity training, and receive targeted emails.
<b>Exercise Resources</b>	CenturyLink performs annual testing through checklist, tabletop, simulation exercise or actual events. The exercise scope ranges from several participants to more than a hundred and from a few hours to multi-day events. Any gaps are identified, documented and tracked to resolution.

**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:

Element	Planning Description
<b>Immediate Actions</b>	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.
<b>Internal Communications</b>	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.
<b>Business Resumption Procedures</b>	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.



# Business Continuity Planning

## An All-Hazards Approach to Maximize Recoverability



Element	Planning Description
<b>External Communications</b>	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.
<b>Vital Resources</b>	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.
<b>Disaster Service Support</b>	CenturyLink retains support for disaster services in the areas of 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.
<b>Mutual Aid</b>	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.
<b>Disaster Recovery Trailers</b>	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.



# Crisis Management

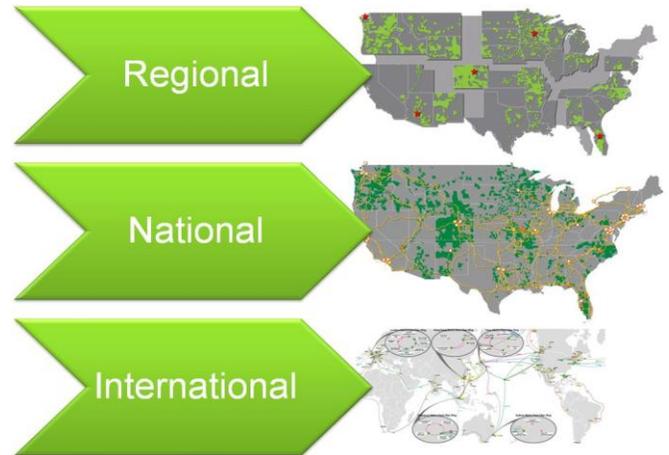
## Rapid Asset Protection, Response and Recovery

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



**Command Centers.** CenturyLink maintains a number of Command Centers to support incident management activities. The corporate Command Center is located in Littleton, Colorado. The Command Center is equipped with multiple media sources, telecommunications diversity, satellite phones, 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. Many are also equipped with satellite phones and HF radio. The corporate Command Center is also equipped with a federal government-sponsored SHARES radio (Shared Resources High Frequency Radio Program).

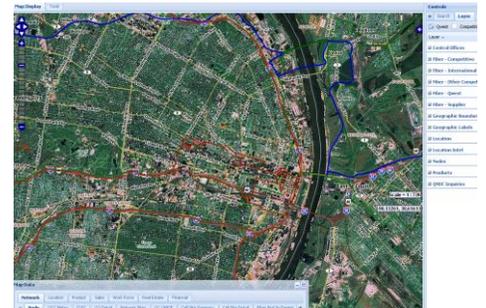
# Crisis Management

## Rapid Asset Protection, Response and Recovery

**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 also has contracts that provide telecommunications-specific support. CenturyLink may use this support for either preventive or responsive measures.



**Geographic Information Systems.** We believe that our crisis management 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.



# Disaster Preparedness Sustainability Environment, Resources and Continuity



**Environmental Sustainability.** Hurricane Sandy drew attention to the increasing climate-related risks for communities and businesses. Disasters are happening more frequently and with greater intensity. CenturyLink supports greening initiatives that aid the environment while aligning with recovery objectives. That's 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.



**Disaster Environment Mitigation.** CenturyLink partnered with local and federal agencies to manage a 1.5 mile area of Cotton Creek, Colorado where severe erosion was threatening a Central Office. Cottonwood Creek was a \$3 million project. This project protects the CenturyLink building, ensures communication for critical facilities and is environmentally responsible.



**Green 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.



For more information, please contact CenturyLink Disaster Preparedness or Crisis Management:

[DPER@CenturyLink.com](mailto:DPER@CenturyLink.com)

