

# 2012 Disaster Preparedness/Business Continuity Program Overview

A CenturyLink White Paper

**“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.”**

**– Mission Statement**



CenturyLink has developed 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 have 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, and updating, and testing. This document summarizes CenturyLink’s crisis management and business continuity program, plans, and related activities.



## Contents

- Disaster Preparedness Governance .....3
- Disaster Preparedness Staffing.....4
- Business Continuity Planning .....5
- Crisis Management .....7

## Disaster Preparedness Governance

### Enterprise Support and Commitment

#### Corporate Policy

CenturyLink has established a corporate policy that 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 are required to acknowledge that appropriate plans have been developed, and to 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. 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. These standards are reflected in Business Continuity, Disaster Recovery, and Crisis Management activities.



#### Best Practices

CenturyLink's program and plans have been developed with the involvement of certified business continuity professionals (MBCP and CBCP), and incorporate best practices acknowledged by Disaster Recovery Institute International (DRII) and 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
- Multiple business resumption options for each critical function
- Consideration of 3<sup>rd</sup> party resources
- Routine plan reviews, updating and testing
- Consistent and integrated planning approach across the enterprise.

## Disaster Preparedness Staffing

### Key Individuals Involved at All Levels



**Executive Team.** CenturyLink's Executive's are responsible for providing C-Suite leadership and direction following a catastrophic event, or an event that may have consequence beyond those typically managed by the Crisis Management Team.



**Disaster Preparedness Staff.** CenturyLink staffs a full-time group of disaster preparedness professionals to oversee and support all elements of the corporate program. Staff members hold CBCP certifications, graduate degrees, and have experience in telecommunications or IT operations.



**Regional Teams.** Six regional CenturyLink teams are lead 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.



**Crisis Management Teams.** 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.



**Departmental Business Continuity Leaders and Planners.** 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.



**IT Disaster Recovery Services.** 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.



**Damage Assessment & Rapid Response Teams.** 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 Operations Center.** CenturyLink's Network Operations organization staffs a 24/7/365 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.



**Environmental Health & Safety Teams.** 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 & Safety staff provides support to the business units and is engaged at all levels during any major events or disasters.

## Business Continuity Planning

### An All-Hazards Approach to Maximize Recoverability

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.

#### Planning Approach

*Enterprise-Wide Scope.* CenturyLink recognizes that large enterprises continually increase in complexity and inter-dependence, 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 inter-dependencies involving both internal and external resources. CenturyLink's plans engage company resources from around the globe for the purposes of continuing critical business functions.

*All-Hazards Planning.* 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.



**Government Services, Inc. invites you to an Open House to see and tour a customized Disaster Recovery Trailer.**

**Friday, November 21** 9:00 AM - 1:00 PM  
10300 Eaton Place  
Fairfax, VA 22030  
Parking Lot

Government Services, Inc. has built a Disaster Recovery Trailer that is tailored to replicate the essential network components of a Private Network. The same can be done to help keep your private network survivable in the event of a natural disaster, or get a critical new site up and working if construction problems may otherwise pose delays.

Drop by at any time between 9:00 AM and 1:00 PM to ask questions of the people who maintain the trailer on a daily basis.

*Strategic Diversity.* 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 & redundancy and 3<sup>rd</sup> party agreements, we believe that our plans enable us to effectively respond to business disruptions, even in light of the uncertain and the dynamic nature of current and potential threats.

*Dedicated Resources.* 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.

*Training & Awareness.* Strategic CenturyLink employees participate in a quarterly disaster awareness meetings, business continuity training, and targeted emails.

*Exercised Resources.* CenturyLink performs annual testing through checklist, tabletop, simulation exercise or actual events. The exercise scope ranges from a couple of participants to over a hundred and from a few hours to multi-day. Gaps are identified, documented and tracked to resolution.

## Disaster Preparedness Program Overview

---

### 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:

*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.

*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.

*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.

*External Communications.* CenturyLink plans describe how the company will communicate with customers, suppliers, contractors, business partners, 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.



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

### Recovery Resources

*Disaster Service Support.* 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.

*Mutual Aid.* CenturyLink has agreements with two major telecommunications carriers 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. The most recent examples of when support was both given and received include the Iowa Flooding and Hurricane Ike.



*Disaster Recovery Trailers.* CenturyLink owns 7 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

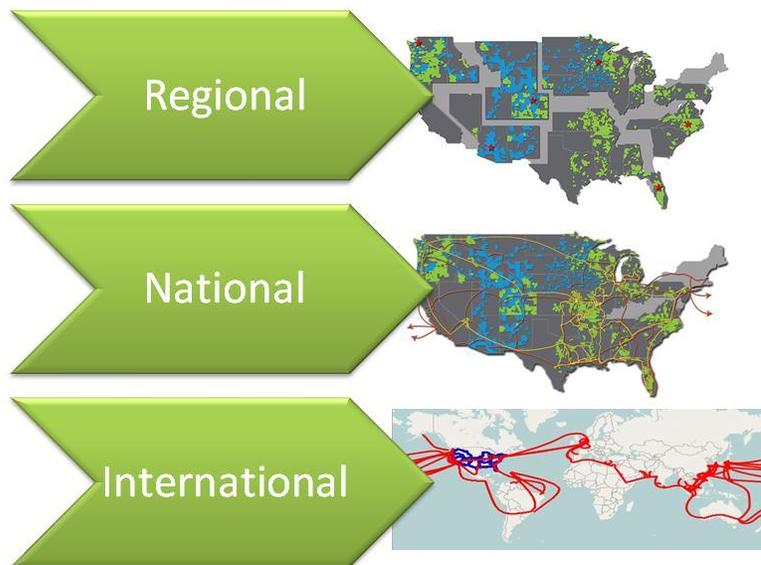
### Rapid Asset Protection, Response, Decision-Making, and Recovery

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 Structure

*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).

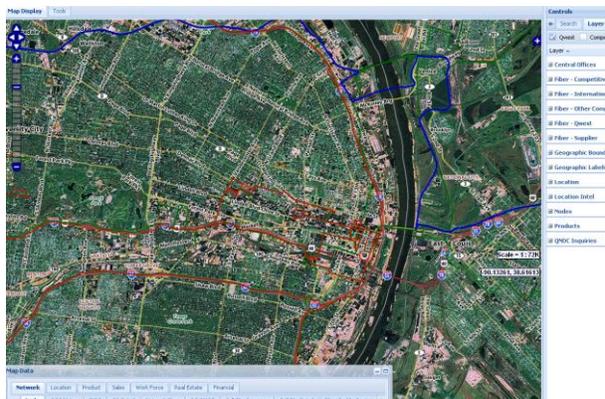
## Disaster Preparedness Program Overview

### 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 24/7/365 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). GIS 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.

