



## BUSINESS CONTINUITY AND DISASTER RECOVERY PLAN

This document describes the Business Continuity and Disaster Recovery processes and activities for DIR or customer initiated and Verizon-initiated Business Continuity and Disaster Recovery Requests in support of the CTSA.

### Business Continuity Teams

Verizon maintains a world-class Business Continuity Program that is essential to the protection of its employees, critical business processes, and structural facilities located around the globe. Verizon is committed to effective response to natural and manmade disasters through its Business Continuity and Emergency Management (BCEM) group. The BCEM organization is the program office for business continuity initiatives world-wide and is chartered to carry out Verizon's core business continuity values. BCEM organizational responsibilities chiefly include:

- **Business Continuity Planning** - Includes risk identification and the coordination of plan development, testing and maintenance.
- **Incident Management** - Where staff members communicate and coordinate, from the various Crisis Management Centers (CMCs) around the globe, the response and recovery efforts for all major disasters.
- **Site Emergency Action Planning** - Site plans developed for all of the corporation's major facilities to include oversight for plan development, training, and evacuation drills.
- **Customer Services Coordination** - Includes RFI/RFP responses, customer presentations, customer consulting, and governmental / regulatory DR interface, as required.
- **Managed Services Coordination** - Includes BC/DR plan development, testing, maintenance, and crisis management for customers that purchase BCEM services.

The BCEM organization is managed and staffed by dedicated industry professionals who are strategically positioned around the globe in North America, EMEA (Europe, Middle East & Africa), and Asia Pacific. These regional teams share a number of objectives - to include a business continuity plan development strategy centered on technical facilities and critical business units, with a heightened sense of focus on the pandemic factors that now influence all BC plan development initiatives. The regional teams also perform in a similar capacity with respect to emergency management and are poised to provide support to any one of several Crisis Management Centers (CMCs) located within their area. By contrast, should any of the regional teams or individual team members be rendered inoperative for any reason, including pandemic causes, team members in other regions are fully capable of standing in and executing a wide array of the critical business continuity functions that are vital to the continued operation of the company.

The entire BCEM team is comprised of business continuity professionals who are certified through either the Business Continuity Institute (BCI) or the Disaster Recovery Institute



International (DRII), and they offer diverse backgrounds in IT, Telecom, business consultancy, emergency management, and business continuance covering all domains of BC / DR best practices.

The Business Continuance and Emergency Management (BCEM) Team manages Business Continuity programs in the Americas region. BCEM coordinates the preparation and implementation of Business Continuity plans, evaluates key indicators to determine potential business impacts to Verizon, and monitors compliance of these plans.

In addition, the BCEM Team provides tactical emergency response and coordinates recovery/restoration activities during major natural disasters, terrorist threats, and incidents involving Hazardous Materials (HazMat) that threaten the stability of the Verizon operations by utilizing the National Emergency Coordinating Center (NECC) and/or MERIT<sup>SM</sup>, Verizon's HazMat Team.

## **Business Continuity**

Business Units in Verizon develop their Business Continuity Program in compliance with the policies contained in the Corporate Business Continuity Program Policy. Verizon's Business Continuity programs involve several areas; Business Impact Analysis (BIA), mitigation, preparedness, activation, response, recovery, restoration, program maintenance, and documentation.

All Verizon Units are responsible for developing, maintaining and testing their Business Continuity plans. Business Continuity plans include the strategies, actions, and procedures required to resume critical and time-sensitive business operations. The plans should be designed to address short-term and long-term business interruptions resulting from natural or manmade events. Business Continuity plans are specific to each business unit and as a minimum include:

- Business Unit Plan Activation
- Business Unit Response Strategy
- Business Unit Recovery Strategy
- Business Unit Restoration Strategy
- Business Unit Resource Inventories

The content of the plan must be kept as concise as possible to allow easy reference in the event of an incident.

Each Business Unit must identify, and document within all Business Continuity plans, the minimum materials necessary to perform critical and time-sensitive business operations. Such materials can include, but are not limited to, software, equipment, supplies, telecom, assets, and vital records.



## **Business Impact Analysis (BIA)**

The Business Impact Analysis (BIA) provides the basis on which Verizon constructs its Business Continuity plans.

The BIA determines the operational impacts resulting from a major disruption of services. It will provide the business unit with:

- The identity of critical and time-sensitive business operations and services
- An analysis of the company's operational impacts
- The time-frames in which critical and time-sensitive operations, processes and functions must resume
- An estimate of the resources necessary for successful recovery and restoration

Verizon's Business Units conduct a BIA at the commencement of their Business Continuity Program, prior to plan development, and annually on an ongoing basis.

## **Mitigation Strategy**

Verizon's mitigation strategy involves the steps taken to either fully prevent or reduce the impact of a business interruption on business operations. Mitigation is the preferred solution to a known risk.

## **Preparedness**

Preparedness is a critical element to continuity planning and involves the activities, programs, and systems developed prior to a business interruption, that are used to support and enhance mitigation of, response to, recovery of, and restoration of business operations.

Elements of preparedness include:

- Communication
- Education and Training
- Evacuation Plans & Training
- Resource Inventories
- Offsite Back-up and Storage of Critical Information
- Annual Exercises/Drills



## **Plan Activation**

Plan activation covers the immediate steps taken to commence a Business Unit's response to scheduled or unscheduled business interruptions.

## **Response Strategy**

A response strategy identifies procedures for:

- Defining the actions to be taken during emergency events to safeguard human life and protect Verizon assets; and
- Reacting to a business interruption caused by an emergency situation.

## **Recovery Strategy**

A recovery strategy identifies procedures for:

- Facilitating and supporting the short-term recovery of critical and time-sensitive business processes;
- Establishing and organizing a command post for recovery operations;
- Mobilizing and activating human and material resources necessary to facilitate and support the recovery process;
- Notifying and appraising critical and time-sensitive product/service recovery team leaders of the situation; and
- Alerting employees, key operational vendors and other internal and external individuals and organizations.

## **Restoration Strategy**

A restoration strategy identifies procedures for:

- Facilitating and supporting the long-term restoration of critical and time-sensitive business processes;
- Facilitating the relocation or migration of business operations to a new or repaired facility;
- Mobilizing operations, support and department relocation or migration; and
- Managing the relocation/migration effort as well as performing employee, key operational vendor, and customer notification before, during, and after relocation or migration.



## **Plan Maintenance**

Plan maintenance methods include:

- Conducting a review of the plan:
  - as a part of the annual Operating Plan (budget) cycle each year
  - when there are significant changes to the operation/organization
- • Updating the plan based on:
  - the results of exercises, drills and testing
  - team members changing assignments or leaving the company

## **Quality Assurance Check**

All Verizon's Business Continuity plans are subject to a mandatory review process. Review includes testing and validation against applicable Verizon Corporate, regulatory, and industry policies and standards.

## **Documentation**

At a minimum, documentation must include:

- A statement of the specific responsibilities of management, staff, special teams and key operational vendors;
- The results of the annual Business Impact Analysis;
- The most current Business Continuity plan, testing schedule, the results of the most recent test for all plan components, and the status of corrective actions;
- Procedures to activate and execute the Response, Recovery and Restoration portions of the plan; and
- The location of vital equipment, tools, assets, data, and records required to execute the Business Continuity plan and maintain business operations.



## Emergency Management

Natural and manmade events that service providers cannot control have the ability to adversely affect communication services. Verizon's dedication to being equipped to rapidly respond to such events is embodied in its culture.

Verizon's use of the "Incident Management System" (IMS), along with the concept of Crisis Management Centers, has greatly enhanced Verizon's control of emergency situations. This process provides a structure that allows for an effective response to any size incident, and maintains flexibility that accommodates those incidents that may escalate in size or impact.

IMS allows all supporting departments to communicate in a structured manner within Verizon as well as with Local, Regional, and National authorities where Verizon responders interact. When faced with the immediate demands of an emergency event, it is essential to have pre-defined processes in place to acquire and deploy the resources needed to overcome any obstacle and ensure a successful event resolution.

Verizon's Incident Management System includes:

- The primary IMS functions are managed by an "Incident Commander" (IC), who oversees the Operations, Planning, Logistics, and Financial Administration of any situation. The IC's focus is to coordinate a consistent corporate interaction with all involved public agencies and media, minimize customer impact, use repair finances/resources in the most cost effective way, and oversee the return of business operations.
- Dynamic structure with flexibility that allows management of events from minor incidents to global catastrophes. Effective for physical network situations, logical "cyber" events, and situations that may impact other business operations.
- Execution not reliant upon any single organization, network platform, product offering, or geographically specific area.
- Key components include interactive network of Emergency Communications Centers (ECC) and Emergency Response Teams (ERT).
- Interfaces with public emergency response agencies.

The procedures contained in the BCEM program reflect Verizon's general procedures implemented when a sudden and unforeseen natural or man-made event impedes our ability to provide communication services within a specific geographic service area. In the event of a disaster that affects the ability of Verizon to provide communications services to its subscriber base, the senior member of the affected facility makes an initial determination of the severity of the emergency and reports the assessment directly to the Global Event Network Management Center (GENMC). The GENMC has processes in place to activate emergency operations procedures.



### Activation of Incident Management System

Any Verizon employee can identify a situation that appears to require full or partial implementation of this plan. This individual will then immediately notify the next level of management, their pre-designated alternate, or the highest-ranking Site Executive immediately available with responsibilities for that specific geographical area. As soon as first notifications are complete, immediate establishment of a local Incident Commander would occur.

At this point, the local Incident Commander informs the Global Event Network Management Center (GENMC) of the situation, and generally provides the following information:

1. The exact nature of the disaster. (e.g. Fire, Flood, Hazmat, Sabotage, Terrorist Activity, Computer/Network Virus, Earthquake, Hurricane, etc.).
2. Identify any known injuries or hazards to employees or others. (If HazMat is involved, then supply all applicable information as required on the Environmental Incident Report).
3. The impact on the network and the subscriber base, (It is helpful to be able to provide type of network impacted, number of lines or a percentage of the total local capacity to assist in assessment of the impact to the overall network).
4. The effect of the disaster on the installed mechanical and electronic equipment.
5. An estimate of the internal resources and time required restoring services.
6. A quick identification of external resources or other support needed.
7. Impact of the disaster on the infrastructure external to Verizon (e.g. Roads, Airport, Power Company, Competitors, Interconnecting Carriers, etc.).

Depending on the size and scope of the event (local, national or global), either a Local Emergency Coordinating Center or the National Emergency Coordinating Center will be activated. Once established, these Emergency Coordinating Centers (ECCs) become the communication “hubs” during an incident. Various communication “bridges” (i.e., conference calls) are essential to the flow of information and are established immediately according to the plan.

Appropriate customer service and public relations contacts are immediately notified of any business interruption affecting Verizon and its customers. In the event of a major incident affecting Verizon customers, the network, or a facility, Verizon will coordinate closely with Local, Regional, and National emergency services personnel to communicate appropriate information. Coordination occurs through a variety of channels including, but not limited to, toll-free customer service lines, public web sites, customer account teams, and the media, as appropriate. Verizon also works with the National Coordination Center (NCC),



Cabinet Office (UK), and other government agencies, in the event government facilities or services are affected, or in the event a government response is needed.

### **National Emergency Coordinating Center (NECC)**

The National Emergency Coordinating Center (NECC) supports Verizon's operations primarily in the United States, in the event of a critical business interruption that exceeds the resource capabilities of a Local Emergency Coordinating Center (LECC) (described below). The NECC is also capable of supporting emergency response activities globally. It is designed to enhance decision-making, communication, coordination, resource allocation, and collaboration between internal member organizations. The Center becomes the main focal point for communications from Executive Management, as well as providing a forum for team status, event progression, and incident resolution. The NECC, located in Richardson, Texas and managed by Verizon's Business Continuity and Emergency Management group, engages in semi-annual functional exercises that are generally 4-8 hours in length.

### **Regional Crisis Management Centers (RCMC)**

The Regional Crisis Management Centers (RCMC) support Verizon operations in the Asia Pacific region. Due to the company's geographical disbursement, several RCMCs are established across the Asia Pacific Region: Hong Kong, Sydney - Australia, and Singapore. The day-to-day operation, implementation, management, and maintenance of each RCMC is a primary responsibility of the Asia Pac Business Continuity Team. When activated, each RCMC is supported by the Regional Crisis Management Team (RCMT) members residing in each location. The RCMT is comprised of primary and secondary points of contact nominated by Regional Executives.

The Regional Crisis Management Team's (RCMT) purpose is to:

- Receive, analyze, and disseminate information about the incident to enable timely decision-making.
- Facilitate the use of Incident Management System (IMS) to enhance communication and coordination efficiencies.
- Enhance decision-making, communication, coordination, resource allocation, and collaboration between member organizations.
- Develop and coordinate the execution of recovery and restoration strategies.
- Provide post-incident reports and recommendations.

### **Emergency Management Control Centers (EMCC)**

The Emergency Management Control Centers (EMCC) support Verizon operations in the EMEA (Europe, Middle East, and Africa) region. Two EMCCs are available for use during an incident. The main center is based in Reading, United Kingdom, with a secondary center available at 4 hours notice in the London area. The EMCC rooms are dedicated management centers equipped with PCs, conferencing facilities and diverse communication (including satellite communication), and have been designed to be used





either in the event existing facilities have been rendered unusable or if a dedicated location requiring people to work in close proximity will aid the response to an incident.

The day-to-day operation, implementation, management, and maintenance of each EMCC are a primary responsibility of the EMEA Business Continuity Team.

In general, each EMCC is utilized for:

- Business Continuity Plan invocation or general / reactive crisis management use.
- Specialist or single business unit response teams.
- Executive or management teams.
- A single point of contact for external authorities / regulators where required.
- To add monitoring or management capacity resources when required externally.
- In addition, each EMCC provides:
  - A dedicated, resilient, purpose built, small office environment with diverse systems, security, and protected mains power, from which incidents can be managed.
  - A workspace, with work docking stations, printer, fax, fixed lines, and satellite phones.
  - Voice conference facilities.
  - Fixed and portable PCs with current corporate images and key data.

#### **MERIT<sup>SM</sup>**

MERIT<sup>SM</sup> is a team of Verizon employees with varying telecommunications backgrounds, who have been trained in performing telecommunications equipment and network repair functions in a hazardous material, contaminated environment.

This team of specialists has been trained under OSHA (Occupational Safety & Health Administration) and NFPA (National Fire Protection Association) guidelines to protect Verizon personnel and assets during times of natural disaster or hazardous materials incidents.

#### **Local Emergency Coordinating Center (LECC)**

The LECC is utilized as a central point of contact to facilitate local communications, logistical support, and information dissemination to key local personnel and ERTs.

LECCs are strategically placed to support of Verizon operations.



## Emergency Response Team (ERT)

The Emergency Response Team is a group of qualified personnel with varying disciplines who have been trained and are responsible for reacting to non-hazardous events that pose a threat to Verizon network operations.

ERTs have been deployed extensively within the Verizon network and provide an excellent supplement to the local workforce. These teams are capable of being deployed at a moment's notice, delivering the job competency necessary to protect and restore the Verizon network in the shortest time possible.

ERTs are strategically placed in support of Verizon operations.

## Tools and Assets

Verizon has developed and implemented several tools and procedures that support both our early warning systems and risk assessment capabilities when it comes to severe weather conditions and natural events. Prior to the activation of any of Verizon's Crisis Management Centers, the Business Continuance & Emergency Management (BCEM) group is responsible for monitoring weather and hazardous conditions around the globe and performs this function 24x7x365.

BCEM utilizes Verizon's in-house weather monitoring process "StormCon", that allows Verizon to leverage multiple sources of weather data to identify potential impact areas and conduct automated pre-storm risk reduction activities. These pre-storm activities help assure that Verizon facilities and personnel are protected during the storm and restoration teams and equipment are staged effectively, ready to respond in the affected area prior-to or immediately after landfall.

Verizon also possesses the ability to effectively 'map' locations down to the one meter level with multiple overlays to include weather data, hazardous locations, transportation data, and more. This capability provides for more timely and enhanced communications. Predictive analysis is also enhanced with respect to resources and facilities prone to damage.

Verizon maintains an inventory of disaster recovery assets for immediate deployment to a disaster impacting the Verizon network. These resources, along with resources from key vendors, provide equipment, temporary shelters, generators, critical communication tools, and supplies necessary for the restoration and recovery of network elements, transmission systems, and customer premise equipment. In a disaster, these resources are deployed as needed in support of local recovery requirements.

During a disaster in the US, Verizon can also utilize the resources of its Big Red Fleet to support the restoration and recovery of the network. The specific mission of the Big Red Fleet is to provide emergency communications and relief personnel for:

- Victims of natural and/or manmade disasters.
- Verizon and our corporate customers, when a disaster affects business operations.



The Big Red fleet consists of 2 semi-tractor trailers and a motor coach with a separate communications equipment trailer. Each vehicle has been converted into a state-of-the-art mobile communications facility offering both VoIP and Internet capabilities. Big Red can be deployed to either US coast within 24 hours.

Verizon in the Americas also maintains a 53-foot Command Trailer to effectively facilitate event management remotely, while further enhancing network restoration and recovery efforts. It's a unique, one-of-a-kind, industry-leading, mobile response and recovery vehicle that houses functional work areas for key recovery functions and is designed to support the implementation of the Incident Management System. Occupants have access to a suite of systems and monitoring tools that will facilitate information gathering and analysis from any location. Communications capabilities inside the Command Trailer are as good as or better than most permanent communications centers.

Verizon also maintains and routinely deploys several other mobile assets purposely designed and built for the zero-infrastructure environment. These units provide field personnel with temporary living accommodations and other facilities that address basic human needs following a deployment to a disaster area.

All of these teams, resources, and assets are maintained by Verizon at a level of readiness to respond quickly and efficiently in the event of a disaster. Verizon conducts regular training, holds disaster exercises, regularly maintains disaster recovery documentation, and performs preventative maintenance on all recovery assets and support tools to assure a high level of readiness.

### **Network Security Incident Response Team (NSIRT)**

Due to the size of Verizon's computing environment, protocol dictates that responses to Information System disruptions are well planned, timely, and efficient. The Network Security Operations Center (NSOC) provides for effective responses to information system security incidents of varying sizes and complexity. The NSOC uses a variety of contacts to address disruptions, such as internal help desk assistance, external vendors, and industry forums.

Verizon's Network Security Incident Response Team (NSIRT) responds to major information system security incidents that are unexplained, affecting multiple systems and/or multiple platforms, occurring in multiple locations, occurring repeatedly or for which a First Response Organization is unable to resolve the incident.

The Network Security Operations Center is responsible for the activation of the team and overall management of the incident until resolution.