

**LOCAL CABLE SYSTEM**

**MODEL DISASTER RECOVERY PLAN**

**&**

**INCIDENT RESPONSE MANUAL**

**Developed by the Communications Security,  
Reliability and Interoperability Council Working  
Group 2-B**

March 14, 2011

## Document Status

**Table 1: Document Status**

<b>Document Control Number:</b>				
<b>Document Title:</b>				
<b>Revision History:</b>				
<b>Date:</b>				
<b>Responsible Author:</b>				
<b>Status:</b>	Work in Progress	Draft	Issued	Closed

**Table 2: Key to Document Status Codes**

<b>Work in Progress</b>	An incomplete document, designed to guide discussion and generate feedback that may include several alternative requirements for consideration.
<b>Draft</b>	A document in a format considered largely complete, but lacking review by all essential personnel. Drafts are susceptible to substantial change during the review process.
<b>Issued</b>	A stable document, which has undergone rigorous review and is suitable for implementation and testing.
<b>Closed</b>	A static document, reviewed, tested, validated, and closed to further change requests.

**Table 3: Master Distribution List**

<b>Name</b>	<b>Title</b>	<b>Contact</b>	<b>Date Issued</b>
		<b>Office:</b> <b>Home:</b> <b>Cell:</b>	

## Table of Contents

Document Status .....	ii
Introduction.....	1
Objectives .....	2
Definition of Terms .....	5
Document Distribution .....	7
Procedures .....	7
DRP Maintenance .....	8
Scheduled Maintenance.....	8
Unscheduled Maintenance.....	9
DRP Testing .....	10
Responsibility for Establishing Testing Scenarios .....	10
Scope and Type of Plan Testing .....	10
Structured walkthrough. ....	11
Site-Specific exercise.....	11
Schedule of Plan Testing .....	11
Plan Testing Announcements .....	12
Test Scenarios .....	12
Evaluation of Plan Testing.....	13
Plan Testing History .....	14
Prevention .....	15
Vulnerability Assessment Guidelines .....	17
Emergency Procedures .....	18
Job Responsibilities .....	18
Incident response team.....	18
Management. ....	19
Staff. ....	20

Personnel Authorized to Declare an Emergency.....	20
Initial Assessment .....	21
Incident Command Center .....	22
Evacuation Procedures .....	23
Guidelines. ....	23
Key Contacts.....	25
Incident Response Team.....	25
Employee. ....	26
Corporate. ....	26
Media. ....	27
Suppliers and Vendors.....	27
Medical and Emergency.....	28
Generator.....	28
Facility maintenance. ....	29
Utilities. ....	29
Communications .....	30
Internal.....	31
External.....	32
Recovery Strategies .....	33
Bibliography.....	38
References Cited in This Document.....	38
Suggested Reading and Other Resources.....	38
Appendix A: Pandemic Preparedness.....	40
Appendix B: Incident Response Manual.....	43
Appendix C: Cable System Vulnerability Assessment Checklist.....	46
Appendix D: Incident Command Center Inventory Template.....	51
Appendix E: Emergency Evacuation Plan Template .....	53
Appendix F: Survey Form Template .....	61

## List of Figures

Figure 1: Basic Recovery Planning Steps .....	2
---	---

## List of Tables

Table 1: Document Status.....	ii
Table 2: Key to Document Status Codes.....	ii
Table 3: Master Distribution List .....	iii
Table 4: DRP Test History.....	14
Table 5: Incident Command Center Location .....	22
Table 6: Incident Response Team .....	25
Table 7: Employee Contact Information .....	26
Table 8: Corporate Contact Information .....	26
Table 9: Media Contact Information.....	27
Table 10: Suppliers and Vendors .....	27
Table 11: Medical and Emergency Contacts .....	28
Table 12: Government Contacts.....	29

## Introduction

The core of this document is the result of the Media Security and Reliability Council which was chartered by the FCC to prepare a comprehensive national strategy for securing and sustaining broadcast facilities throughout the United States during attacks, natural disasters and all other threats nationwide.

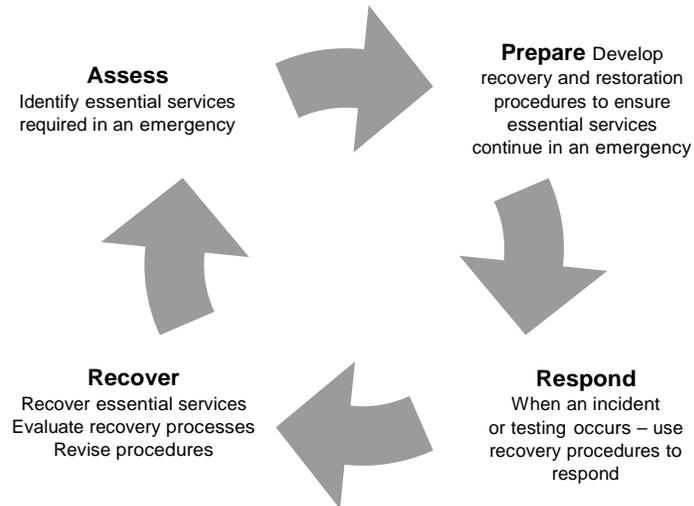
Changes in technology required that this document be updated for The Communications Security, Reliability and Interoperability Council to assure optimal reliability, robustness and security. As of this date the MSRC I and MSRC II documents can be found at <http://www.mediasecurity.org>.

Disaster recovery planning is a practical approach to contingency and risk management designed to reduce the consequences associated with an extended disruption of essential services. The scope of this document is to provide guidelines to develop a short term Disaster Recovery Plan (DRP) and Incident Response Manual (IRM) (Appendix A) for use as a tool by your organization for the timely resumption of essential services in emergency situations. Long-term Disaster Recovery plans, and business recovery issues, while important, are beyond the scope of this document. This document is generic in nature, and is designed to serve as a template. **[Cable system]** is encouraged to adapt its use to accommodate any unique requirements that may exist.

**As you formulate your disaster recovery plans you should ask yourself what you would do in the event your facility and all of the day-to-day operational resources you use were no longer available.**

## Objectives

Figure 1 shows the basic disaster recovery planning steps that should be followed in order to ensure that the timely recovery of essential services is initiated in the event of an emergency situation.



**Figure 1: Basic Recovery Planning Steps**

The objective of this document is to provide guidelines and strategies that will allow [Cable system] to effectively accomplish these steps by assessing the vulnerability and impact to critical systems, and to recover operations and essential services in the event of a disruption caused by a natural or man-made disaster or other emergency situations in an organized and efficient manner. To meet these objectives the DRP should address the following major topics:

- Vulnerability assessment and prevention.
- Plan distribution and maintenance.
- Staff roles and responsibilities.
- Essential equipment, materials and services.
- Internal and external communications.
- Recovery strategies and procedures.
- Periodic plan testing.

In the event of an incident, it is essential to ensure that proper levels of notification and communication regarding the event are disseminated to personnel, emergency services and other stakeholders.

**It should be recognized that any plan should be flexible enough to be adapted to the particular emergency situation. The key to recovering from an emergency situation, with minimum impact, is to have a DRP and to follow it.**

## Requirements

When developing the DRP guidelines, the following requirements should be met:

- All processes critical to the continuation of essential services should be identified.
- Critical personnel should be identified and receive the plan.
- The plan should be reviewed no less than annually
- The plan should be tested.
- Availability of emergency information to the deaf and hard of hearing.
- Availability of emergency information to non-English speaking persons.

- Establish and maintain lines of communication with industry and governmental forums assisting with DRP (e.g. NCC, ESF2, NRSC, ATIS)

## Definition of Terms

The following terms and abbreviations are used throughout this document.

**Disaster** – For purposes of this document, a disaster is an event that creates an inability for an organization to provide essential services. Disasters are typically classified into these basic types:

- Natural – wind, rainstorms, hurricanes, tornadoes, cyclones, volcanic eruptions, earthquakes etc.
- Man-made – fire, explosions, release of toxic fumes, vandalism, sabotage, burst pipes, building collapse, bomb threats, equipment failure, airplane crash, etc.
- Civil disorder – resistance to authority such as riots, terrorist activities, etc.
- Cyber Security- Attacks to the information and communications infrastructure

**Disaster Recovery Plan** – The approved written plan used to develop processes and prepare the resources, actions, tasks, and data required to facilitate recovery from any disaster or emergency.

**Disaster Recovery Planning Manager** – The individual or individuals assigned to oversee the creation, implementation, testing, periodic review and distribution of the DRP.

**Emergency Evacuation Coordinator** – The individual or individuals assigned to oversee the creation, implementation, testing, periodic review and distribution of the Emergency Evacuation Plan.

**Emergency Evacuation Plan** – A written plan that communicates the policies and procedures for personnel to follow in the event an emergency situation requires vacating a facility.

**Emergency Evacuation Team** – A group of individuals that develops and executes the policies and procedures for vacating a facility as required in the event of an emergency situation. The group consists of the Emergency Evacuation Coordinator, Safety Monitors, Disaster Recovery Planning Manager, Incident Response Team, and representation from other departments.

**Incident Command Center** – The central gathering location for the Incident Response Team to facilitate the emergency communication process by enabling quick and clear exchanges of information for decision-making.

**Incident Response Manual** – A task oriented document for the use in the timely resumption of an organization's essential services in emergency situations

**Computer Security Incident Response Team** – Personnel identified in advance as part of the disaster recovery effort. They are selected based on their skills and knowledge of the various IT operations within the organizations. This team has the responsibility to ascertain the level of response needed during an emergency, and coordinate the recovery process.

**Incident Response Team** – Personnel identified in advance as part of the disaster recovery planning effort. They are selected based on their skills and knowledge of the various operations within the organizations. This team has the responsibility to ascertain the level of response needed during an emergency, and coordinate the recovery process.

**Master Distribution List** – The record of personnel who are to receive a copy of the DRP.

**Recovery** – Recovery pertains to the immediate reinstatement of an organization's essential services after a natural or man-made disaster or other emergency situation.

**Safety Monitor** – The individual or individuals whose primary responsibility it is to check assigned areas to ensure that occupants have vacated a facility in the event of an evacuation.

**DRP** – Disaster Recovery Plan

**EEP** – Emergency Evacuation Plan

**ICC** – Incident Command Center

**IRM** – Incident Response Manual

**NOC** – Network Operations Center

## Document Distribution

This section describes the procedures for distributing the DRP.

### Procedures

The Disaster Recovery Planning Manager is responsible for the distribution of the DRP, as well as any additional emergency procedures as applicable. The DRP document should be distributed to the Incident Response Team (see Table 6) and others listed on the Master Distribution List (see Table 3). Copies should also be kept in the following locations:

**Master Hard Copy** – The original printed version of the DRP that is used to generate subsequent copies. A hard copy of the DRP should be located in the local Disaster Recovery Planning Manager's office.

**Master Soft Copy** – The original electronic version of the DRP that is used to generate subsequent copies. An electronic copy of the DRP should be stored on a storage device that is backed up routinely.

- **Distribution Copy #2** – A copy of the DRP should be kept at each facility if separate facilities are used.
- **Distribution Copy #3** – A copy of the DRP should be kept at the Customer Support, Network Operations Center (NOC), and Dispatch facilities.
- **Distribution Copy #4** – A copy of the DRP should be kept at a secure off-site location.
- **Distribution Copy #5** – When applicable, a copy of the DRP should reside at a Division or Corporate office.
- **Distribution Copy #6** – Two copies of the DRP should reside at the Incident Command Center (ICC) (see Table 5).

**The DRP contains proprietary company information and is not for general distribution. Each individual possessing a copy is responsible for maintaining it in a secure location, and in accordance with company policies for the protection of proprietary information. The Disaster Recovery Planning Manager is responsible for maintaining the DRP in an updated condition and distributing the revised document whenever the DRP is updated.**

## **DRP Maintenance**

This section describes the procedures for maintaining the DRP. Maintenance procedures consist of two general categories: scheduled and unscheduled. Scheduled maintenance is time-driven, where unscheduled maintenance is event-driven.

### **Scheduled Maintenance**

Scheduled maintenance consists of a scheduled annual review and updates as well as an annual structured walkthrough and tactical exercises.

Scheduled maintenance occurs as the result of a scheduled review of the plans. Reviews are predictable and are scheduled not less than annually. The purpose of the review is to determine whether changes are required to strategies, tasks, notifications and assembly procedures.

The Disaster Recovery Planning Manager is responsible for initiating Scheduled Maintenance activities. The Disaster Recovery Planning Manager should initiate reviews twice yearly. The Incident Response Team and their alternates should review the strategies and procedures for changes that may be required. The reviews should address events that have occurred within each team members' area of responsibility that may affect prevention, response, and recovery capability.

The Disaster Recovery Planning Manager is responsible for any required updates to the DRP that results from the review. The Disaster Recovery Planning Manager should import all changes to the master hard copy, print hard copies of the plan, redistribute the copies as described above, and ensure that all issued copies are updated to the same level as the master hard copy.

**Ongoing consideration should be given to how the DRP will be maintained and stored in a secure and reliable manner. The DRP should be available to the key personnel under all circumstances.**

### **Unscheduled Maintenance**

Certain maintenance requirements are unpredictable and cannot be scheduled. The majority of these unscheduled plan changes occur as the result of major changes to hardware or software, network configurations, personnel changes, etc. The following are examples of items that may trigger the need for unscheduled maintenance:

- Significant modifications in the physical plant (i.e., changes in equipment or equipment locations, network operating software, changes to signal routing, changes in IT based local area or wide area networking connectivity etc.).
- Changes in on-site and off-site storage facilities (i.e. Parts and equipment storage lockers, sheds, closets....think about both physical and data storage).
- Changes in major operations facilities (i.e. Headend, Hub, NOC, etc.).
- Significant modification of business or operational support systems (i.e. Traffic and billing systems, Conditional access systems, etc. Anything that integrates with and affects day-to-day technical operations).
- Transfers, terminations, promotions, personnel relocations (i.e. home telephone and/or cell telephone number changes) or resignations of individuals from the Incident Response Team.
- Recent acquisition of or merger with another company.
- Textual alert delivery that relies on IT specific resources or IP integration with 3<sup>rd</sup> party delivery mechanisms

The Disaster Recovery Planning Manager should be made aware of all potential changes to the plans resulting from unscheduled maintenance. The Disaster Recovery Planning Manager should meet with the personnel submitting the change and update the DRP as necessary.

### **DRP Testing**

This section describes the procedures for periodically testing the DRP.

#### **Responsibility for Establishing Testing Scenarios**

The Disaster Recovery Planning Manager and the Technology Manager (Title will vary depending on the company such as Chief Engineer, Director of Engineering, etc. should meet with all department heads named in the Master Distribution list to develop testing for each department. For example, the Disaster Recovery Planning Manager and the Lead Maintenance Technician should meet to identify all critical system power supplies and compose testing scenarios for each.

At first, a block diagram of all major subsystems can be developed, then as the plan matures; smaller subsystems can be included in the testing scenarios.

The input of all affected parties, including non-technical personnel should be requested so that routine tasks essential to the normal operations of the system are not overlooked.

While conducting DRP testing, it is essential to carefully document events as they occur during the test, noting unexpected, unusual or abnormal systems operation. Be aware of the amount of time and stress factors involved in carrying out DRP testing scenarios. It is recommended that an engineering staff member or assistant be assigned the task of keeping a log during the test. This will be of assistance during the review of the test to refine and improve performance in subsequent testing.

#### **Scope and Type of Plan Testing**

Conducting periodic tests of the DRP is mandatory to ensure that plans meet the recovery needs defined by the organization. These tests should be structured so as to be realistic without disrupting the normal business process. Testing should be planned, organized and conducted in such a way that results can be documented, verified, and evaluated.

Disasters can happen in many ways, some unimaginable and unforeseeable. Developing a testing scenario for each and every disaster may not be possible. The Disaster Recovery Planning Manager should make every effort to identify all types of disasters likely to occur in their locality and then imagine other disasters that may occur, though only rarely. All disaster testing scenarios should be based on worst-case conditions.

During the testing of the DRP it may not be possible to duplicate the actual conditions of a disaster for test purposes. For example, while conducting a test of the DRP for a complete evacuation of a facility, say for a bomb threat, the actual physical evacuation of personnel and customers may not be practical because of the business disruption that will result from the test.

**For some testing a simulation can be used. For example, if the test for that day is a complete building evacuation; non-critical personnel can assemble at their assigned meeting point, or, if the facility is in a high-rise building, a simulated assembly area might be the elevator lobby on the tested floor. The testing team would then interview the staff to make certain they know what procedures to follow in the event of an actual building evacuation.**

### **Structured Walkthrough**

A structured walkthrough is the first step in developing a testing strategy and may consist of gathering department heads and touring the facility to identify critical areas of concern. Each department head can identify the critical systems in their area of responsibility while noting comments from others about interoperability issues. A priority list of testing of all major systems and subsystems can then be developed.

### **Site-Specific Exercise**

Some locations may require site-specific exercises. The plans and testing for the main facilities may not work for other locations. Testing and planning needs to be customized for all locations.

### **Schedule of Plan Testing**

It is required that a schedule be developed for testing each critical system and subsystem. For example, the “power failure at essential facilities” test might be scheduled during the night to avoid potential interruption of essential services. Critical systems should be tested more often than ancillary subsystems. The Disaster Recovery Planning Manager may require “damage to essential facilities” testing every three months, while “damage to physical plant” testing may be performed only once or twice per year. The DRP in its entirety should be tested no less than annually.

Some testing, for example, emergency generator power systems, should be done regularly, and tested annually with all power fully disconnected from the utility power grid. This will verify that all critical systems are connected to the correct emergency backup power supply.

### **Plan Testing Announcements**

Announcements of major system and subsystem testing should be given far enough in advance to allow for proper steps to be taken in preparation for the test. For example, if the Headend's backup generator is to be tested, engineering personnel should make sure that all critical systems are fully backed up and redundant. Steps should be taken in case the tested system fails the scheduled test to make sure that there are no unplanned interruptions to essential services. In a typical environment, a 7 to 10 day advance notice of DRP plan testing should be sufficient.

After the DRP is developed, consideration should be given to preparing an annual schedule of systems and subsystems testing. This will assist engineering personnel in planning maintenance tasks and upgrades to either coincide with or avoid DRP testing parameters.

**In the event of an actual disaster, it is critical that a complete event log be kept to allow for a later review of recovery efforts and any changes that may improve those procedures.**

### **Test Scenarios**

When composing the test scenario, consideration should be given to the complexity of the test, how much time it will take to perform the test, how much time it will take to properly de-brief and evaluate the test, and the general impact of the test on normal day to day operations of the facility. Also, if the test includes change out of equipment and/or changes to normal signal path routing, care should be taken to restore the tested system to pre-test configuration. It is recommended that careful system configuration notes and photos be taken before the test is conducted to ensure that the system can be restored to normal operations.

## Evaluation of Plan Testing

As each segment of the DRP is tested, an evaluation should be conducted to identify problem areas in both the testing scenario and the recovery strategy. The following questions will help serve as a guide for evaluating the efficacy of the conducted tests:

- Did the testing run smoothly?
- Did the test run through all the steps to conclusion?
- Is the test practical?
- Does the test show that the planned recovery strategy is functional?
- Does the test interfere with other systems or departments not included in the test?
- Does the test interfere with the delivery of services?
- At the conclusion of the test was a return to normal operations easily accomplished?

After completion of the test a series of meetings should be held with the affected departments, as well as the Incident Response Team, Emergency Evacuation Team in order to compile observations, comments, and criticisms and give each participant a chance to recommend if necessary changes to the plan. The Disaster Recovery Planning Manager should then update the plan and redistribute the revised plan.

It may be necessary to re-test the same segment of the plan multiple times before all concerned departments agree upon a testing protocol. Proper planning, testing and implementation of recovery strategies will facilitate a fast and complete return to “normal” operations during an emergency.

**Remember, it is much easier to solve problems in the light of day than in the fog of war.**

## Plan Testing History

DRP testing should be carefully documented to provide a complete record of events as the plan is maintained and updated. The plan testing history will then provide an accurate record of test results, evaluations and updates as well as a record of when each test segment of the plan was carried out. The Disaster Recovery Planning Manager can use the test history as a tool to determine what changes may have occurred if a test suddenly no longer works. A log for documenting the test results is provided in Table 4.

**Table 4: DRP Test History**

Date	Tester	Test Type	Test Results

## Prevention

### Vulnerability Assessment Guidelines

To facilitate the assessment of vulnerabilities that potentially may exist in **[Cable system]**, a model Cable System Vulnerability Assessment Checklist developed by the Media Security and Reliability Council is provided in Appendix B (Media Security and Reliability Council, 2005). The Media Security and Reliability Council (“MSRC”) is a Federal Advisory Committee, formed by the Federal Communications Commission, to study, develop and report on communications and coordination designed to assure the optimal reliability, robustness and security of the broadcast and multi-channel video programming distribution industries in emergency situations.

The checklist is not intended to be comprehensive, and **[Cable system]** is encouraged to adapt its use to accommodate any unique requirements that may exist. The Vulnerability Assessment Checklist should be reviewed and updated as necessary but no less frequently than annually. The following guidelines are also provided as a tool to help facilitate the assessment of vulnerabilities that potentially may exist. **[Cable system]** is encouraged to review and follow these guidelines:

- Redundancies that are planned to provide adequate protection against equipment failure and even natural disasters are not necessarily the same as those needed to protect against a deliberate attack. Specifically, protection against deliberate attack requires security measures at facilities and a combination of both redundancy and geographic diversity for critical equipment and facilities.
- Disaster recovery plans should be periodically updated, tested and rehearsed.
- Vulnerability assessments should consider the location and geographic distribution of key facilities in the market, such as Headends and Hubs.
- Cable operators in a region should collaborate, where possible, to increase their collective site and equipment diversity, redundancy and interconnections.

- Cable systems and local broadcasters in a region should work jointly to develop prevention plans and to improve the redundancies in their interconnections.
- Cable systems should plan IT disaster recovery procedures for sourcing replacement infrastructure (routers, switches, firewalls), servers, computers and software media needed to restore, operate the facility of operation. Data services for communication such as e-mail, Internet access, and critical data files should be coordinated with IT recovery.
- Appropriate measures to be taken to provide redundant and geographically diverse equipment for their Headend, Hub, Internet-based connectivity, and plant facilities, appropriate to the system's operations and facilities.
- Redundant signal routes should extend as far out in the network as economically practical.
- Where economically feasible, the physical plant should be appropriately "hardened," particularly in areas prone to severe weather or natural disasters.
- Essential equipment and service suppliers should be examined to ensure that critical resources would have sufficient capacity and delivery capabilities to meet needs during an emergency. This is particularly important where fuel for backup generators is concerned. **[Cable system]** should consider securing arrangements for fuel deliveries from suppliers located outside of the local market during emergency situations.
- **[Cable system]** should coordinate with federal, state and local authorities to ensure that technical and operations personnel are properly credentialed and recognized so they can carry out recovery procedures and gain access to essential facilities and equipment during times of emergencies.
- **[Cable system]** should coordinate with power and communications entities to ensure that essential facilities and equipment are given an adequate priority level with respect to repair and recovery schedules.

- **[Cable system]** should use available resources to notify subscribers of estimated recovery times.
- **[Cable system]** should establish plans to communication status to local, state, and federal entities.

## Emergency Procedures

This section discusses the basic steps that should be followed in order to ensure that the timely recovery of essential services is initiated in the event of an emergency situation.

### Job Responsibilities

#### Incident Response Team

- Help to ensure the health and safety of all personnel.
- Coordinate and assist in all response and recovery efforts.
- Ensure all disaster recovery methods and procedures conform to **[Cable system]** policies.
- Ensure that the DRP is periodically reviewed and updated.
- Ensure that the DRP is periodically tested and rehearsed.
- Ensure that local and regional management is contacted concerning the emergency, and is provided periodic updates on recovery efforts.
- Assist management in communications with **[Cable system]** personnel.
- Coordinate communications with essential equipment and service suppliers, including contract construction and installation personnel, utility providers, fuel providers (diesel, propane, gasoline, etc.) and external telecommunications and Internet providers, to ensure the availability of critical resources.
- Facilitate meetings required during and following an emergency. Distribute meeting agendas, minutes, status and action items to team members and personnel. Report all information/status to management.
- Ensure that necessary repair and reconstruction materials can be obtained if there is an anticipated shortage in-house.
- Ensure that alternative methods to communicate with key field personnel in the event that radio, cell systems or other primary methods are inoperable.

## Management

- Ensure the health and safety of all personnel.
- Ensure appropriate credentialing of personnel.
- Ensure that the [Cable system] DRP is implemented as specified.
- Assist in response and recovery efforts.
- Ensure that sufficient cash reserves are available in the event that banks and ATMs are inaccessible.
- Ensure that adequate alternate facility(s) are available in the event that the emergency situation dictates that primary facility(s) should be evacuated.
- Ensure that primary and alternate facilities are secure.
- Ensure that adequate food, water, and housing is available to personnel and their families if necessary.
- Ensure that counseling is available to personnel.
- Ensure adequate and secure long-term parking for personnel.
- Coordinate communications with **[Cable system]** personnel, local government officials and media.
- Establish accountability for local, state, and federal reporting.
- Ensure that the necessary resources are available to the Incident Response Team so that the **[Cable system]** DRP can be updated, tested, and implemented as specified.
- Ensure that personnel are familiar with the **[Cable system]** DRP.
- Ensure that there are reciprocal agreements with other cable operators and local broadcasters.

## **Staff**

- Be familiar with the DRP, and help ensure it is implemented as specified.
- Perform initial damage assessment as outlined in the DRP in a safe and secure manner.
- Assist in response and recovery efforts.
- Report any potential or actual emergency situation to the Incident Response Team and Management.
- Seek medical attention for any health problems caused by the emergency situation.
- Identify equipment and personnel needs and report those needs to the Incident Response Team and Management.
- Communicate location and status to the Disaster Recovery Planning Manager, Incident Response Team or Management on predetermined basis during emergency situations, particularly after an evacuation occurs.
- Install or oversee the installation of new or replacement hardware and software.
- Test or oversee the testing of new or replacement hardware and software to ensure proper functionality.

## **Personnel Authorized to Declare an Emergency**

It is the responsibility of each employee to address emergency situations in accordance with the DRP in the event that they are aware of a situation that could result in a disruption in **[Cable system]** operations and delivery of essential services. An emergency event may not require that the entire DRP be implemented. The Incident Response Team and Management should evaluate each event on its impact and severity.

## Initial Assessment

The individual(s) discovering or responding to the emergency situation should follow these general guidelines. If possible and time permits, the following assessment process should occur:

- Assess the situation. Consider your safety a top priority.
- If applicable, inform co-workers and customers of the situation.
- If necessary, evacuate the facility. Protect vital records and perform emergency response; i.e. contain fire, power down operations equipment, etc.
- When applicable, place calls to obtain the appropriate assistance from local authorities, i.e., 911, etc.
- Document who has been called and their response.
- Notify the applicable Incident Response Team member. Be prepared to provide the following information, when applicable, to the personnel that are contacted:
  - Nature of the emergency, and time of the occurrence.
  - Extent of damage to facilities and/or plant.
  - Current status of the emergency situation including what is being done to confine or rectify problem.
  - Resources which may be needed from a Corporate, Division, or Regional office.
  - Members of the Incident Response Team who have been contacted.
  - The local authorities that have been contacted.
  - The best method to contact you.
  - The Disaster Recovery Planning Manager and applicable members of the Incident Response Team will convene to determine a solution and strategy for recovery.

It is the responsibility of each employee to address emergency situations in accordance with the DRP in the event he/she is aware of a situation that could result in a disruption in operations and the delivery of essential services. An emergency event may not require that the plan be implemented. The Incident Response Team, Disaster Recovery Planning Manager, or Management should evaluate each event on its impact and severity.

**Incident Command Center**

The ICC is a location or locations identified in the planning process for the Incident Response Team to operate from in the event of an emergency. The ICC could simply be an area within the organization’s facilities, such as a conference room, or a designated external location. The ICC will be at the location(s) identified in Table 5.

**Table 5: Incident Command Center Location**

<b>Primary Locations</b>	<b>Address</b>	<b>Contact</b>
<b>Secondary Locations</b>	<b>Address</b>	<b>Contact</b>

Regardless of where it is located, the ICC should have a backup power source, phones, radio and television receivers, and any other communication systems as needed including computers for email and access to the Internet. Personnel should be assigned the responsibility of ensuring that the ICC contains adequate supplies for a 48-72 hour period, and that those supplies are periodically rotated and maintained. **[Cable system]** may also wish to consider acquiring security services for the ICC to protect essential equipment and assets. An example Inventory Checklist for the ICC is provided in Appendix C:

**As you develop plans for your facilities in the event of an emergency, you should ask yourself what resources would be needed for the next 48-72 hours?**

## **Evacuation Procedures**

This section is designed to assist **[Cable system]** personnel in the creation of an emergency response process for the protection of life and physical assets in the event of a fire, explosion, chemical spill or any emergency requiring a facility evacuation. An Emergency Evacuation Plan (EEP) template for customization by **[Cable system]** is provided in Appendix D.

### **Guidelines**

- A site Emergency Evacuation Team should be identified. The team should consist of an Emergency Evacuation Coordinator, as well as Safety Monitors as appropriate for each floor of the site with the appropriate number of male and female searchers for each of the floors in the site. The Disaster Recovery Planning Manager and Incident Response Team should be identified as members of this team. Alternates should be assigned as appropriate.
- The Emergency Evacuation Team should be cross functional with representation from other departments such as Advertising, Communication, Construction, Customer Support, Facilities, Human Resources, Installation, Legal, Network Operations Center (NOC), information technology (IT), Marketing, Technical, Warehouse.

- Floor plans with the evacuation routes and any relevant evacuation information should be posted on each floor (at several locations on the floor). This information should also be included in the EEP.
- Designate meeting sites at a location outside your site providing sufficient distance to ensure the safety of personnel and visitors.
- Review your operations to determine which critical operating systems may require continuing attention or shutdown during an evacuation or other emergency situation. Develop a procedure to ensure that requisite actions are taken during an emergency. Ensure that you have designated personnel to address these issues, provided them with the procedure, and trained them in its use.
- Train the Emergency Evacuation Team on their responsibilities to implement the plan and to assist in the safe and orderly emergency evacuation of the facilities.
- Ensure that you have a procedure in place for communication and evacuation/safe refuge of disabled persons.
- Develop personnel responsibilities lists. Ensure that affected personnel are familiar with individual and group responsibilities.
- Determine methods and procedures for essential recovery personnel, including the Incident Recovery Team, Disaster Recovery Planning Manager, engineering, operations, and technical staff members to communicate their location and status on predetermined bases after evacuation occurs.
- Develop a training program for distribution and review by personnel.
- Coordinate the EEP with the **[Cable system]** DRP and IRM.
- Conduct periodic practice evacuations and evaluate the outcome of those drills.
- Update the plan annually.

## Key Contacts

### Incident Response Team

The Incident Response Team is a group of employees identified in advance during the disaster planning process. They are recruited based on their skills and knowledge of the various operations within the organizations. This team has the responsibility to ascertain the level of response needed during an emergency, and coordinate the recovery process. These individuals should also have alternates identified in the event the primary member is not available to perform their duties. This can be as simple as the General Manager and the department heads of the facility, with assistant department heads as the alternates. All members of the Incident Response Team should carry a photo ID or other recognized credentials in order to carry out recovery procedures and gain access to essential facilities and equipment during times of emergencies. Members of the Incident Response Team are listed in Table 6.

**Table 6: Incident Response Team**

Name	Title	Contact	Responsibilities
		Office: Home: Cell:	

## Employee

A list of active employees is available in Table 7. All personnel should carry a photo ID.

**Table 7: Employee Contact Information**

Name	Title	Contact	Responsibilities
		Office: Home: Cell:	

## Corporate

A list of key corporate contacts is listed in Table 8.

**Table 8: Corporate Contact Information**

Name	Title	Contact	Responsibilities
		Office: Home: Cell:	

## Media

In the event that an emergency situation requires coordination with the local Radio, Newspaper, Television, and other media contacts are listed in Table 9.

**Table 9: Media Contact Information**

Company Information	Representative	Contact
		Office: Home: Cell:

## Suppliers and Vendors

Table 10 lists the various suppliers and vendors that may be used during recovery. Suppliers and vendors assisting recovery efforts on site should carry a photo ID or other recognized credentials in order to gain access to essential facilities and equipment.

**Table 10: Suppliers and Vendors**

Company Information	Representative	Contact
		Office: Home: Cell:

Prior to being selected a supplier should be qualified. For example, in a blackout, if a supplier of diesel fuel does not have emergency power, they may not be able to pump fuel into their trucks for arrival to your facility.

### Medical and Emergency

Table 11 lists the contact information for local police, fire and medical assistance.

**Table 11: Medical and emergency contacts**

Company	Address	Contact
		Office: Home: Cell:

### Generator

Company Information	Representative	Contact
		Office: Home: Cell:

**Facility Maintenance**

Name	Title	Contact	Responsibilities
		Office: Home: Cell:	

**Utilities**

Company Information	Representative	Contact
		Office: Home: Cell:

**Table 12: Government Contacts**

Name	Title	Contact	Agency
		<u>Office:</u> <u>Home:</u> <u>Cell:</u>	

## **Communications**

Effective communications can be a challenge during the extreme intensity of a disaster or emergency situation. Whatever the circumstances, the goal of communications during and after emergencies will be the rapid and accurate collection and dissemination of information so that lives may be saved, injuries minimized, fears allayed, and essential services and operations recovered quickly and effectively.

**[Cable system]** is encouraged to develop and implement a communications strategy in advance that meets the needs of everyone affected during a disaster or emergency situation. Consideration should be given to the functions needed to perform in an emergency and the communications systems needed to support them.

## ***Internal***

During and after emergencies, it will be necessary to communicate with **[Cable system]** personnel concerning what actions need to be taken and other vital information. The Disaster Recovery Planning Manager and Incident Response Team will be the central coordinative link for such communications. These employees and other personnel involved in recovery procedures should be equipped with cell phones, two-way radios, satellite phones, ham radios, text messaging capabilities (e.g., "Blackberries"), or similar devices so that they may communicate with each other effectively in real time during an emergency. It is critical that **[Cable system]** has multiple means of communicating reliably with personnel during an emergency and not depend upon any single method.

During recovery efforts, essential recovery personnel, including the Incident Recovery Team, Disaster Recovery Planning Manager, and other engineering, operations, and technical staff members should communicate their location and status on predetermined bases.

E-mail may also be an effective means of coordination among the Incident Response Team before, during and after and disaster, or other emergency situation. **[Cable system]** should consider creating e-mail distribution lists so that e-mail messages are broadcast to all members of the lists. Utilize an external email service in the case where internal email is completely unavailable. Consider development of an offsite Disaster Portal where people can check in by entering an update of their own location. These messages could contain notifications about where to meet, task responsibilities, resources that may be needed or other information pertaining to the emergency.

If phones are operative, communications to personnel at home and at work will be handled by attempting initially to contact personnel directly using the employee contact information contained in Table 7. In this situation a voice mail system can also be used to inform personnel of the status of the worksite. If this is unsuccessful, or if the phones are not operative, communications to personnel may be made using two-way radios, satellite phones, ham radios, e-mail, and messenger system as deemed appropriate, until such time as the normal phone service resumes. In some cases, announcements can also be provided to the radio, television, and print media. Personnel should be informed in advance whenever this type of resource will be utilized and directed to the one that will be used to provide information about **[Cable system]**.

Effective planning should take into account that personnel will need to know whether their families are safe during an emergency, and likewise, families will want to know that the staff member is safe at the facility. However, personnel should refrain from tying up telephone lines and thereby impeding necessary communications. During an emergency, [Cable system] may wish to establish a toll-free number, web site or other means for family members to use to receive a status update.

## **External**

During an emergency situation, it is critical to communicate quickly, accurately and perhaps frequently to a variety of external audiences, such as the media, local authorities and municipalities, including franchise authorities, federal agencies (e.g., FCC, FEMA, etc.) elected officials, opinion leaders, customers, and suppliers. Complete mandatory and voluntary reports for entities such as public utility commissions, Federal Communications Commission (NORS outage reports and DIRS).

During and after emergencies, these external entities may frequently contact **[Cable system]**. These contacts may be general inquiries, requests for sensitive information, requests for assistance, or may be for the purpose of exchanging information of mutual interest. To ensure that communication is ongoing and shared with those entities touched by the emergency, it is essential that all such contacts be immediately directed to the local Public Information Officer, Public Affairs staff, Legal department, or other entity serving as the focal point for these external communications.

**[Cable system]** may also wish to consider placing messages pertaining to the emergency situation on voice mail or Automated Response Units so that the public can access information pertaining to the emergency situation, and consider activating emergency alert systems. The Federal Communications Commission encourages cable operators to transmit emergency alerts as a public service.

To facilitate the gathering of information that may be needed by external entities, a survey form template is provided in Appendix E. The template is not intended to be comprehensive, and **[Cable system]** is encouraged to adapt its use to accommodate any unique situation that may exist.

## Recovery Strategies

All recovery plans should start with an assessment of the vulnerabilities within **[Cable system]**. It is the responsibility of the Disaster Recovery Planning Manager to work with **[Cable system]** personnel to identify specific risks, threats, incidents or situations that may impact ongoing system operations, and to define the steps to be taken to prevent (Vulnerability Assessment), react (Contingency Plan), and respond (Incident Response Plan), to these events as they occur. These plans are not meant to be long term restoration efforts, but rather guidelines to get essential services to the customer as quickly as possible.

After the vulnerability assessments are complete and documented, further planning can take place to develop strategies and solutions to minimize the vulnerabilities and risks identified should they be encountered. It is essential that responsibility for each area of concern be assigned to qualified personnel. It is also essential that the plan be tested and practiced under realistic conditions to reveal any weaknesses that may not be initially apparent.

There is nearly an infinite number of natural or man-made disaster or other emergency situations which could occur including bomb threats, earthquakes, fires, flooding, gas leaks, hurricanes, tornados, snow storms, etc. However, while there are any number of situations which could occur, the associated vulnerabilities and risks can generally be grouped as follows:

- The loss of the use of all or critical portions of the facility.
- Loss of the transmission facilities.
- Loss of access to facilities.

As such, it does not matter why the loss of use or access to a facility occurs. For example, access to the main facility might be lost due to a hazardous atmosphere, a local law enforcement action or any number of other emergency situations. What does matter is the availability of a flexible set of strategies and plans that are well thought out in advance of the situation. They must be practiced and tested periodically, used alone or in groups, to rapidly recover from the emergency.

Problems that **[Cable system]** could potentially encounter due to an emergency situation include:

- Power failure at essential facilities such as a Dispatch, Headend, Hub or NOC.
- Power failure in the physical plant.
- Damage to essential facilities or physical plant.
- Lock down - personnel cannot leave the facilities.
- Mandatory evacuations.
- Personnel cannot access the facilities or into the building(s).
- Loss of telephony wired/wireless.
- Loss of data networking capabilities.
- Loss of communications capabilities to field personnel.
- Satellite receive failures.
- Lawlessness.

Below are just two examples of the many guidelines and procedures you will need for proper planning in the event of these types of problems. **[Cable system]** is encouraged to define additional guidelines and procedures to accommodate additional, as well as any locally unique, emergency situations using similar forms in this section. Planning for different geographic locations is also required. Planning for earthquakes in Southern California is a requirement, but planning for snowstorms is not.

**Example: Power Failure at the Headend**

Recovery	Preparation	Responsibility	Procedures
<p>Arrangements should be made for the periodic unattended delivery of generator fuel, and alternate sources for generator fuel, including outside of the local market, which can be obtained on short notice.</p>	<p>Procedure should be documented for manually switching to backup power.</p> <p>Consider redundant fuel systems for generator (e.g., natural gas and diesel)</p>	<p>[Outline each area of responsibility and have qualified staff to accomplish the tasks necessary]</p>	<p>Ensure generator has started and is functioning properly; manually start generator if necessary.</p>
<p>Maintain alternate sources for portable generators that can be obtained quickly.</p>	<p>Backup generator should be tested routinely under typical loading conditions while disconnected from commercial power.</p>		<p>Monitor generator fuel consumption, and ensure generator is routinely fueled and maintained.</p>

### Example: Power Failure in the Physical Plant

Recovery	Preparation	Responsibility	Procedures
Maintain alternate sources for portable generators and batteries that can be obtained quickly.	Standby batteries should be properly maintained and tested to ensure they are fully operational under load.	[Outline each area of responsibility and have qualified staff to accomplish the tasks necessary]	Ensure system power supply is functioning properly. Manually switch to batteries if necessary.
Arrangements should be made for the periodic delivery of portable generator fuel, and alternate sources for portable generator fuel which can be obtained on short notice.	System power supplies should be tested to ensure they automatically switch to batteries during a power outage.		Verify proper voltage and RF signal levels; monitor battery standby time.
Arrangements should be made for portable generator security (e.g. chain, padlock, security guard,	Procedures should be documented for operating system power supply from a portable generator.		Switch to portable generator in the event standby time is exceeded.
Coordinate recovery efforts and schedules with power utility.			Ensure portable generator is secured, and routinely fueled and maintained.

### Example: Damage to Physical Plant

Recovery	Preparation	Responsibility	Procedures
Assess plant conditions such as nodes without commercial power; extent of damaged to fiber, trunk, feeder; etc.	Maintain redundant and diverse signal routes from Headends to Hubs. Perform routine testing of redundant routes.	[Outline each area of responsibility and have qualified staff to accomplish the tasks necessary]	Assemble tools and equipment and begin plant recovery efforts  Order of plant recovery: <ul style="list-style-type: none"> <li>• Facilities</li> <li>• AC Power</li> <li>• Fiber</li> <li>• Distribution</li> <li>• Drop</li> </ul>
Determine amount of external resources, such as construction contractors, necessary to help minimize duration of recovery efforts.	Maintain sufficient quantity of spare plant equipment (e.g., active and passive devices, fittings, strand and cable, etc).		Ensure portable generators are secured, and routinely fueled and maintained.
Continue outage assessment throughout the recovery efforts so that work is not routed to areas that can't be restored in a reasonable period of time.	Copies of plant design maps should be accessible by restoration personnel.		Implement security and traffic control measures; maintain personal and public safety throughout restoration efforts.

## Bibliography

### References Cited in This Document

Media Security and Reliability Council. (2005, September 19). *Local cable system model vulnerability assessment checklist*. Retrieved September 19, 2005 from <http://www.mediasecurity.org/documents/CableVulnerabilityChecklist.pdf>

### Suggested Reading and Other Resources

American Radio Relay League. <http://www.arrl.org/>

Barnes, P., & Hiles, A. (1999). *The definitive handbook of business continuity management*. New York: John Wiley & Sons.

Barnes, J.C. (2001). *A guide to business continuity planning*. New York: John Wiley & Sons.

Blythe, B. T. (2002). *Blind sided: A manager's guide to catastrophic incidents in the workplace*. New York: Portfolio Hardcover.

Bullock, J.A., & Haddow, G.D. (2003) *Introduction to emergency management*. Burlington, MA: Butterworth-Heinemann.

Cohn, R. (2000). *The PR crises bible: How to take charge of the media when all hell breaks loose*. New York: Truman Tally Books.

Department of Homeland Security, (2005, September 19). *Preparing America*. Retrieved September 19, 2005 from [http://www.dhs.gov/dhspublic/theme\\_home2.jsp](http://www.dhs.gov/dhspublic/theme_home2.jsp)

Elliot, D., Herbane, B., & Swartz, E. (2001) *Business continuity management*. New York: Routledge.

Federal Communications Commission. <http://www.fcc.gov/>

Federal Emergency Management Agency. <http://www.fema.gov/>

Fink, S. (2000). *Crises management: Planning for the inevitable*. New York: Authors Guild.

- Hiles, A. (2003). *Business continuity: Best practices (2nd ed.)*. Brookfield, CT: Rothstein Associates.
- Laye, J. (2002). *Avoiding disaster: How to keep your business going when catastrophe strikes*. New York: John Wiley & Sons.
- Media Security and Reliability Council. (2005, September 19). *Adopted best practice recommendations*. Retrieved September 19, 2005 from [http://www.mediasecurity.org/documents/MSRC\\_I\\_Best\\_Practices.doc](http://www.mediasecurity.org/documents/MSRC_I_Best_Practices.doc)
- Media Security and Reliability Council. (2005, September 19). *MSRC documents*. Retrieved September 19, 2005 from <http://www.mediasecurity.org/documents/>
- Mitroff, I.I. (with Anagnos, A.). (2000). *Managing crises before they happen*. New York: American Management Association.
- National Association of State EMS Directors. <http://www.nasemsd.org>
- National Cable and Telecommunications Association. <http://www.ncta.com>
- Network Cable and Telecommunications Association. <http://www.nasemad.org>
- Toigo, J. (2003). *Disaster recovery planning: Preparing for the unthinkable (3<sup>rd</sup> ed.)*. Upper Saddle River, NJ: Prentice Hall PTR
- Wallace, M., & Webber, L. (2004). *The disaster recovery handbook: A step-by-step plan to ensure business continuity and protect vital operations, facilities, and assets*. New York: American Management Association.

## **Appendix A: Pandemic Preparedness**

Health and Human Services, the Centers for Disease Control and Prevention and OSHA have developed guidelines, including checklists, to assist businesses, industries, and other employers in planning for a pandemic outbreak. This document will reference their recommendations and provide links to the plans developed by these organizations. Pandemic preparedness should be part of every disaster recovery plan.

### **From the OSHA documentation:**

To reduce the impact of a pandemic on your operations, employees and the general public, it is important for all businesses and organizations to include continuity planning for a pandemic. Lack of continuity planning can result in a cascade of failures as employers attempt to address challenges of a pandemic with insufficient resources and employees who might not be adequately trained in the jobs they will be asked to perform. Proper planning will allow employers to better protect their employees and prepare for changing patterns of commerce and potential disruptions in supplies or services.

Develop a disaster plan that includes pandemic preparedness, review it regularly and conduct drills.

- Be aware of and review federal, state and local health department pandemic influenza plans. Incorporate appropriate actions from these plans into workplace disaster plans.
- Prepare and plan for operations with a reduced workforce.
- Work with your suppliers to ensure that you can continue to operate and provide services.
- Develop a sick leave policy that does not penalize sick employees, thereby encouraging employees to stay home so that they do not infect other employees. Recognize that employees with ill family members may need to stay home to care for them.
- Identify possible exposure and health risks to your employees. Are your employees expected to have a lot of contact with the general public?
- Minimize exposure to fellow employees or the public. For example, will more of your employees work from home? This may require enhancement of technology and communications equipment.
- Identify business-essential positions and people required to sustain business-necessary functions and operations. Prepare to cross-train or develop ways to function in the absence of these positions.

- It is recommended that employers train three or more employees to be able to sustain business-necessary functions and operations, and communicate the expectation for available employees to perform these functions if needed during a pandemic.
- Plan for downsizing services but also anticipate any scenario that may require a surge in your services.
- Recognize that, in the course of normal daily life, all employees will have non-occupational risk factors at home and in community settings that should be reduced to the extent possible. Some employees will also have individual risk factors that should be considered by employers as they plan how the organization will respond to a potential pandemic (e.g. immunocompromised individuals and pregnant women).
- Stockpile items such as soap, tissue, hand sanitizer, cleaning supplies and recommended personal protective equipment. When stockpiling items, be aware of each product's shelf life and storage conditions. Make sure that your disaster plan protects and supports your employees, customers and the general public. Be aware of your employees' concerns about pay, leave, safety and health. Informed employees who feel safe at work are less likely to be absent.
- Develop policies and practices that distance employees from each other, customers and the general public. Consider practices to minimize face-to-face contact between employees such as e-mail, websites and teleconferences. Policies and practices that allow employees to work from home or to stagger their work shifts may be important as absenteeism rises.
- Work with your employees and their union(s) to address leave, pay, transportation, travel, childcare, absence and other human resource issues.
- Provide your employees and customers in your workplace with easy access to infection control supplies, such as soap, hand sanitizers, personal protective equipment (such as gloves or surgical masks), tissues, and office cleaning supplies.
- Provide training, education and informational material about business-essential job functions and employee health and safety, including proper hygiene practices and the use of any personal protective equipment to be used in the workplace. Be sure that informational material is available in a usable format for individuals with sensory disabilities and/or limited English proficiency. Encourage employees to take care of their health by eating right, getting plenty of rest and getting a seasonal flu vaccination.

- Work with your insurance companies, and state and local health agencies to provide information to employees and customers about medical care in the event of a pandemic.

Assist employees in managing additional stressors related to the pandemic. These are likely to include distress related to personal or family illness, life disruption, grief related to loss of family, friends or coworkers, loss of routine support systems, and similar challenges. Assuring timely and accurate communication will also be important throughout the duration of the pandemic in decreasing fear or worry. Employers should provide opportunities for support, counseling, and mental health assessment and referral should these be necessary. If present, Employee Assistance Programs can offer training and provide resources and other guidance on mental health and resiliency before and during a pandemic.

Below are several suggested websites that you can rely on for the most current and accurate information:

[www.flu.gov](http://www.flu.gov)

(Managed by the Department of Health and Human Services; offers one-stop access, including toll-free phone numbers, to U.S. Government avian and pandemic flu information.)

[www.osha.gov](http://www.osha.gov)

(Occupational Safety and Health Administration website)

[www.cdc.gov/niosh](http://www.cdc.gov/niosh)

(National Institute for Occupational Safety and Health website)

[www.cdc.gov](http://www.cdc.gov)

(Centers for Disease Control and Prevention website)

## Appendix B: Incident Response Manual

The objective of the Incident Response Team manual is to ensure that critical contact information necessary to ensure the timely resumption of service is available quickly to the Incident Response Team in the event of an emergency. The contents of this manual are included in the [Cable system] DRP in various locations and sections are duplicated here. It is intended that team members at all times carry the Incident Response Manual. Questions and/or suggestions concerning this manual should be directed to the Disaster Recovery Planning Manager.

The following information is currently included in this Manual:

- Incident Response Team contact information.
- ICC location and backup location.
- Contact information for selected personnel.
- Contact information for selected suppliers and vendors. Contact information for local police, fire and medical assistance.

**Table 1: Incident Response Team**

Name	Title	Contact	Responsibilities
		Office: Home: Cell:	

## Incident Command Center

**Table 2: Incident Command Center Location**

<b>Primary</b>	<b>Address</b>	<b>Contact</b>
<b>Secondary Locations</b>	<b>Address</b>	<b>Contact</b>

## Employee Contact Information

**Table 3: Employee contact information**

<b>Name</b>	<b>Title</b>	<b>Contact</b>	<b>Responsibilities</b>
		<b>Office:</b> <b>Home:</b> <b>Cell:</b>	

## Selected Suppliers and Vendors

**Table 4: Selected Suppliers and Vendors**

<b>Company Information</b>	<b>Representative</b>	<b>Contact</b>
		<b>Office:</b> <b>Home:</b> <b>Cell:</b>

## Medical and Emergency

**Table 5: Medical and Emergency Contacts**

<b>Company</b>	<b>Address</b>	<b>Contact</b>
		<b>Office:</b> <b>Home:</b> <b>Cell:</b>

## Appendix C: Cable System Vulnerability Assessment Checklist

The following vulnerability assessment checklist is provided as a tool for use by **[Cable system]** to help facilitate the assessment of vulnerabilities which potentially may exist in the system. This checklist is not intended to be comprehensive, and **[Cable system]** is encouraged to adapt its use to accommodate any unique requirements that may exist.

<b>Disaster Recovery Plan</b>		
Does a Disaster Recovery Plan exist that details how to effectively assess impact to the facilities and recovery operations in the event of an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the Disaster Recovery Plan identify essential personnel necessary to carry out restoration efforts?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the Disaster Recovery Plan describe the Recovery Time Objective (RTO) to establish the backup origination facility in the event of an emergency and for how long the backup origination can be sustained?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the Disaster Recovery Plan include other ways for network or other programming to be received?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the Disaster Recovery Plan include agreements to gain assistance from other broadcast, cable and production operations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the Disaster Recovery Plan include reciprocal agreements with other local broadcasters to allow multi-channel rebroadcast of signals on DTV in the event of a loss of transmission capability?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the Disaster Recovery Plan identify essential equipment and service suppliers, including contract engineers, construction and installation companies, fuel, and external telecommunications providers, to ensure availability of critical resources?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the Disaster Recovery Plan include alternative methods to communicate with key field personnel in the event that radio, cell systems or other primary methods are inoperable?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Does the Disaster Recovery Plan include data restoration and offsite backup of program and playback software (restoration of data includes servers, remote control systems, telephones, and routers)?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Is the Disaster Recovery Plan periodically reviewed and updated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
Is the Disaster Recovery Plan periodically tested and rehearsed?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

<b>Pandemic Preparedness</b>			
<b>Workforce</b>	Have you prepared for operating with a reduced workforce?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Have you identified the possible exposure and health risks to your employees?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Have you identified business-essential positions and cross trained employees to sustain operations?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Have you considered policies that allow for certain employees to work from home?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Infection control</b>	Have you stockpiled soap, tissue, hand sanitizer, cleaning supplies and recommended personal protective equipment?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Have you provided informational material about employee health and safety?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

<b>Headend and Hub Facilities</b>			
<b>Backup</b>	Does the primary Headend facility have backup power?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is Headend backup power automatically activated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Can Headend backup power operate long enough to implement your recovery plan?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are Headend backup power capabilities routinely tested under load?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is the Headend disconnected from commercial power during backup power capability testing?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Do Hub facilities have backup power?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is Hub backup power automatically activated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Can Hub backup power operate long enough to implement your recovery plan?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are Hub backup power capabilities routinely tested under load?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

	Is the Hub disconnected from commercial power during backup power capability testing?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Do you have adequate fuel supplies for generators?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Do you have a portable generator plan to augment back-up power?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Security</b>	Are security protocols sufficient to prevent unauthorized access to the Headend and Hub facilities?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

<b>Emergency News &amp; Information</b>	Can the system obtain news and information from a studio, local franchise authority or local television broadcast signal (e.g., ENG/SNG trucks or satellite links, Internet) in the event of an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the capability exist to provide some news or information from a location other than the primary Headend in an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Can Emergency Alert System ("EAS") messages be received and transmitted from a location other than the primary Headend in an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Do backup facilities exist to receive a signal feed from at least one local television or radio broadcaster in the event the primary means of reception fails?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Backup Equipment</b>	Is spare equipment (e.g., antennas, equipment racks, cable, distribution amps, combiner/splitters, signal processors, etc.) available in sufficient quantities in the event of an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are copies of Headend and Hub cabling diagrams accessible by essential personnel in the event of an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are backup copies of essential software applications and data available in the event of an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

<b>Physical Plant</b>			
<b>Backup Power</b>	Where applicable, are the standby batteries in system power supplies fully operational?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Can backup power operate long enough to implement your recovery plan?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are the standby batteries periodically maintained and tested under load?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are portable generators available in the event standby time is exceeded?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are the backup power systems routinely tested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Where backup power is available is it automatically activated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Does the system employ diverse power grid sources where feasible?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Redundant Signal Routes</b>	Do redundant signal routes exist from Headends to Hubs?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	If yes, do these redundant routes include diverse paths?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are the redundant routes routinely tested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Where applicable, do redundant signal routes exist from Hub to nodes?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	If yes, do these redundant routes include diverse paths?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are the redundant routes routinely tested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Where applicable, do redundant signal routes exist from Headend or Hub to local franchise authorities?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	If yes, do these redundant routes include diverse paths?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are the redundant routes routinely tested?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Backup Equipment</b>	Is spare plant equipment (e.g., active and passive devices, fittings, strand and cable, etc) available in sufficient quantity in an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are copies of plant design maps accessible by essential personnel in the event of an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

<b>Business Systems</b>			
	Are there documented Diversity, Redundancy and Business Continuity Plans regarding your Mission-Critical Business Systems (e.g., Traffic, Log and Billing, Broadcast Automation, Media Asset Management Systems, News Desk Computing Systems, Nielsen Measurement and Research Systems, Promotion/Publicity Systems, etc.) including, RTO and how long can these systems be sustained once implementing your Business Continuity Plans?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

<b>Customer Support Facilities</b>			
<b>Backup Power</b>	Do customer support facilities, including NOC, have backup power?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is backup power automatically activated?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Can backup power operate long enough to implement your recovery plan?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Is the customer support facility standby power capabilities routinely tested under load?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Security</b>	Are security protocols sufficient to prevent unauthorized access to customer support facilities?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
<b>Backup Equipment</b>	Does the capability exist to divert calls to an alternate customer support facility in the event of an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No
	Are backup copies of essential operations and customer support systems available in the event of an emergency?	<input type="checkbox"/> Yes	<input type="checkbox"/> No

## Appendix D: Incident Command Center Inventory Template

Category	Item	Quantity	Location
<b>Food</b>	Cook stove/fuel		
	Paper towels		
	Aluminum foil		
	Plastic wrap		
	Paper plates		
	Forks/spoons/knives		
	Cooler		
<b>Water</b>	Drinking		
	Washing		
<b>Lighting</b>	Flashlights		
	Batteries		
<b>Radio/TV</b>	Radios (battery)		
	Batteries		
	TV (battery)		
	Batteries		
<b>Facilities</b>	Beds		
	Bedding		
	Towels		
	Personal hygiene		
	First aid kit		
<b>Data Network</b>	PC		
	Laptop		
	Wireless router		
	Ethernet switch		
	Broadband access		
	Dial-up modem		
	Dial-up access		
<b>Voice Network</b>	Cellular phones		
	Analog/fax lines		

Category	Item	Quantity	Location
<b>Documentation</b>	DRP/IRM	2 copies	
	Facility	2 copies	
	Network		
<b>Tools</b>	Basic hand tools		
	Hardhat		
	Coveralls		
	Duct tape		
	Shop vacuum		
	Broom		
	Dust pan		
	Gloves		
	Rubber boots		
	Safety glasses		
	Fire Extinguisher		
	Sheet plastic		
<b>Office Supplies</b>	White board		
	Dry erase markers		
	Paper pads		
	Pens/pencils		

**Appendix E: Emergency Evacuation Plan Template**

**Department Name:** \_\_\_\_\_

**Site Name:** \_\_\_\_\_

**Site Address:** \_\_\_\_\_

**Emergency Evacuation Coordinator:**  
\_\_\_\_\_

**Emergency Evacuation Coordinator Contact Information:**  
\_\_\_\_\_  
\_\_\_\_\_

**Designated Meeting Site(s) for This Facility are:**  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

**Plan Prepared By:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Emergency Contact Information**

**Fire:** \_\_\_\_\_

**Medical:** \_\_\_\_\_

**Police:** \_\_\_\_\_

**Incident Command Center:**  
\_\_\_\_\_

## Section I: Purpose and Objectives

Potential emergencies at **[Cable system]** such as fires, explosions, hazardous material spills, chemical releases and all other emergency situations may require personnel to evacuate a facility. An EEP and adequate occupant familiarity with a facility minimize threats to life and property. This plan applies to all emergencies where personnel may need to evacuate for personal safety.

This EEP is intended to communicate the policies and procedures for personnel to follow in an emergency situation. This written plan should be made available, upon request, to personnel and their designated representatives by the Emergency Evacuation Coordinator for the facility.

Under this plan, personnel will be informed of:

- The plan's purpose.
- Preferred means of reporting fires and other emergencies.
- Emergency escape procedures and route assignments.
- Procedures to be followed by personnel who remain to control critical plant operations before they evacuate.
- Procedures to account for all personnel after an emergency evacuation has been completed.
- Rescue and medical duties for those staff members who perform them.
- The alarm system.

**[Name/title]** is the Emergency Evacuation Coordinator for this facility and has overall responsibility for the preparation and implementation of this plan.

**[Name/title]** is the Alternate Emergency Evacuation Coordinator.

The Emergency Evacuation Coordinator, in coordination with the Disaster Recovery Planning Manager, will review and update the plan as necessary. Copies of this plan will be maintained in/at: **[location]**

## Section II: General Guidelines

The following guidelines apply to this EEP:

- All personnel should be trained in safe evacuation procedures. Refresher training is required whenever the employee's responsibilities or designated actions under the plan change, and whenever the plan itself is changed.
- The training may include use of floor plans and workplace maps that clearly show the emergency escape routes included in the EEP. Colorcoding aids personnel in determining their route assignments. Floor plans and maps should be posted at all times in main areas (i.e. stairwells, lobbies, elevator lobbies, exit corridors) of **[Cable system]** to provide guidance in an emergency.

- Stairwells are the primary means for evacuation. Elevators are to be used only when authorized by a fire or police officer.
- Personnel will not be permitted to re-enter the facility until advised by the Fire Department.

This EEP will be coordinated with efforts in connected facilities. Mutually beneficial agreements can be reached regarding designated meeting sites and shelter in the event of inclement weather.

### **Section III: Responsibilities of Emergency Evacuation Coordinator and Safety Monitors**

#### **The Emergency Evacuation Coordinator is responsible for:**

- Obtaining and posting floor plans and route evacuation maps.
- Overseeing the development, communication, implementation and maintenance of the overall EEP.
- Ensuring the training of occupants, Safety Monitors, and critical operations personnel, and notifying all personnel of changes to the plan.
- Maintaining up to date lists of occupants, critical operations personnel, and any other personnel with assigned duties under this plan.
- In the event of an emergency, relaying applicable information to the Disaster Recovery Planning Manager, building occupants and Safety Monitors.
- Establishing designated meeting sites for evacuees.
- In coordination with the Disaster Recovery Planning Manager, assist in posting the EEP in work areas, communicating plan to occupants, and updating the plan annually.

#### **The Safety Monitors are responsible for:**

- Assisting in familiarizing personnel with emergency evacuation procedures.
- Acting as liaison between management, the Disaster Recovery Planning Manager, and the Incident Response Team, and their work area.
- Ensuring that occupants have vacated the premise in the event of an evacuation and for checking assigned areas.
- Knowing where their designated meeting site is and for communicating this information to building occupants.
- Having a list of personnel in their area of coverage to facilitate a head count at their designated meeting site.

- Ensuring that disabled persons and visitors are assisted in evacuating the facility.
- Evaluating and reporting problems to the Emergency Evacuation Coordinator after an emergency event.

#### **Section IV: Alerting Occupants in Case of Fire or Other Emergency**

- In case of a fire, personnel should activate the nearest fire alarm box and/or contact the local fire department. Fire alarm box locations are noted on the evacuation floor plans in Section X. The alarm will serve as an alert to building occupants for the need to evacuate.
- It may be necessary to activate additional fire alarm boxes or shout the alarm if people are still in the facility and the alarm has stopped sounding or if the alarm does not sound. This can be done while exiting.
- Persons discovering a fire, smoky condition, or explosion should pull the fire alarm box. Any pertinent fire or rescue information should be conveyed to the Fire Department. All emergency telephone numbers are listed at the beginning of this EEP.
- State your name, your location, and the nature of the call. Speak slowly and clearly. Wait for the dispatcher to hang up first. On occasion the dispatcher may need additional information or may provide you with additional instructions.

#### **Section V: Evacuation Procedures for Facility Occupants**

- When the fire alarm sounds, all personnel should ensure that nearby personnel are aware of the emergency, quickly shutdown operating equipment, close doors, and exit the facility using stairwells.
- All occupants should proceed to their Designated Meeting Site and await further instructions from their Safety Monitor, Emergency Evacuation Coordinator, Disaster Recovery Planning Manager, or Incident Response Team member.
- All personnel should know where primary and alternate exits are located and be familiar with the various available evacuation routes. Floor plans with escape routes, alternate escape routes, exit locations and designated meeting sites are located in Section X and are posted in the facility.
- Occupants should NOT use elevators as an escape route in the event of a fire.

**Notes and precautions:**

- Small fires can be extinguished more effectively if you are trained to use a fire extinguisher. However, an immediate readiness to evacuate is essential.
- All fires, even those that have been extinguished, should be reported to the local fire department immediately.
- Never enter a room that is smoke filled.
- Never enter a room if the door is warm to touch.
- **R - Rescue:** When you discover a fire, rescue people in immediate danger if you can do so without endangering yourself. Exit via a safe fire exit. Never use elevators. Close doors to rooms with fire.
- **A - Alarm:** Sound the alarm by pulling a firebox and call 911 from a safe distance to notify fire command center of precise location of fire.
- **C - Confine:** Close all doors, windows and other openings.
- **E - Evacuate:** Evacuate the facility.

**Section VI: Disabled Occupants**

If a disabled occupant is unable to exit the facility unassisted, the Safety Monitor should notify the emergency response personnel of the individual's location. Transporting of disabled individuals up or down stairwells should be avoided until emergency response personnel have arrived. Unless imminent life-threatening conditions exist in the immediate area occupied by a non-ambulatory or disabled person, relocation of the individual should be limited to a safe area on the same floor, in close proximity to an evacuation stairwell.

## Section VII: On-Air Operations

Critical operations, including equipment that should be shut off or set-up to operate unattended, and persons designated to complete these actions are identified in Table 1. Procedures for these transition activities should be predetermined for life safety and loss control purposes, as well as ensuring complete evacuations in a timely manner.

**Table 1: Critical Operations**

Operation	Required	Name	Contact
			Office: Home: Cell:

The shutdown procedure to be followed by those employees who have been assigned to care for essential **[Cable System]** operations include: On-air; News Studio Operations; News Gathering; Sales and Human Resources.

Individuals involved in these transition procedures should be notified by management of this responsibility in advance. They should be identified in the EEP, and appropriately trained for the particular situation. Of course alternate personnel should be identified as well.

## Section VIII: Accountability Procedures for Emergency Evacuation

Groups working together on or in the same area should meet outside and away from the facility in the prearranged designated meeting site. A list of the primary and alternate designated meeting sites is listed on the floor plans in Section X.

A roster of personnel to ensure that everyone has evacuated has been developed by the Emergency Evacuations Coordinator. The list will be updated whenever there is a personnel change.

Safety Monitors are designated by the Emergency Coordinator and/or the Disaster Recovery Planning Manager and will conduct head counts once evacuation has been completed. There should be at least one Safety Monitor per floor or per twenty occupants to provide adequate guidance and instruction at the time of an emergency.

Personnel selected as Safety Monitors are to be trained in the complete workplace layout and the various primary and alternate escape routes from the workplace. All trained personnel are made aware of employees with disabilities who may need extra assistance and of hazardous areas to be avoided during emergencies. Before leaving, the Safety Monitors are to check rooms and other enclosed spaces in the workplace for other staff members who may be trapped or otherwise unable to evacuate the area, and convey this information to emergency personnel. A list of Safety Monitors and Alternate Safety Monitors for **[Television station]** appears in Table 2.

**Table 2: EEP Contact information**

<b>Responsibility</b>	<b>Name</b>	<b>Location</b>	<b>Contact</b>
<b>Emergency Evacuation Coordinator</b>			<b>Office:</b> <b>Home:</b> <b>Cell:</b>
<b>Alternate Emergency Evacuation Coordinator</b>			
<b>Safety Monitor</b>			
<b>Alternate Safety Monitor</b>			

Once each evacuated group of employees has reached their designated meeting site, each Safety Monitor will:

- Assemble his/her group in the Designated Meeting Site.
- Take head count of his or her group.
- Assume the role of department contact to answer questions.
- Instruct personnel to remain in area until further notice.
- Report status to Emergency Evacuation Coordinator, Disaster Recovery Planning Manager or Management.
- Instruct personnel to remain at designated meeting site until further notice.

**Section IX: Training and Communications**

Each occupant should know that evacuation is necessary and what his/her role is in carrying out the plan. Personnel should also know what is expected of them during an emergency to assure their safety.

A method of training occupants in the requirements of the EEP is to give all personnel a thorough briefing and demonstration. Managers and supervisors should present this plan to personnel in staff meetings. Annual practice drills are to be implemented and documented by the Emergency Evacuation Coordinator and/or Disaster Recovery Planning Manager.

The Emergency Evacuation Coordinator and/or Disaster Recovery Planning Manager should maintain training attendance records.

**Section X: Site Specific Information**

In this Section, the Emergency Evacuation Coordinator, in coordination with the Disaster Recovery Planning Manager, is to insert the following site-specific information:

- Facility Floor Plan
- Primary and Secondary Emergency Evacuation Routes
- Designated Meeting Sites
- Exits
- Fire Alarm Box Locations

## Appendix F: Survey Form Template

### For Each PSID in the Affected Region

PSID: \_\_\_\_\_

Operator: \_\_\_\_\_

Location: \_\_\_\_\_

Name of System: \_\_\_\_\_

### Contact Information

Contact Name: \_\_\_\_\_

Email: \_\_\_\_\_

Phone Number: \_\_\_\_\_

Best Method: \_\_\_\_\_

### System Information

Number of Subscribers Served Before Emergency Situation: \_\_\_\_\_

Number/Percentage of Customers Receiving Service: \_\_\_\_\_

Date System Went Down: \_\_\_\_\_

Projected Date for 25% Service: \_\_\_\_\_

Projected Date for 50% Service: \_\_\_\_\_

Projected Date for 75% Service: \_\_\_\_\_

Projected Date for 95% Service: \_\_\_\_\_

Projected Date for 100% Service: \_\_\_\_\_

