LOCAL RADIO STATION

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

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

Table 2: Key to document status codes

Work in Progress	An incomplete document, designed to guide discussion and generate feedback which may include several alternative requirements for consideration.
Draft	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.
Issued	A stable document, which has undergone rigorous review and is suitable for implementation and testing.
Closed	A static document, reviewed, tested, validated, and closed to further change requests.

Table 3: Master distribution list

Name	Title	Contact	Date Issued
		Office: **Home:** **Cell:**	
		Office: **Home:** **Cell:**	
		Office: **Home:** **Cell:**	
		Office: **Home:** **Cell:**	
		Office: **Home:** **Cell:**	
		Office: **Home:** **Cell:**	

Table of Contents

Document Status ii
Introduction 1
Objectives *1*
Definition of Terms 2
Document Distribution 5
Procedures *5*
DRP Maintenance 6
Scheduled Maintenance *6*
Unscheduled Maintenance *7*
DRP Testing 8
Responsibility for Establishing Testing Scenarios *8*
Scope and Type of Plan Testing *9*
Structured walkthrough. *9*
Site specific exercise. *9*
Schedule of Plan Testing *10*
Plan Testing Announcements *10*
Test Scenarios *11*
Evaluation of Plan Testing *11*
Plan Testing History *12*
Prevention 12
Vulnerability Assessment Guidelines *12*
Emergency Procedures 16
Job Responsibilities *16*
Incident Response Team. *16*
Management. *16*
Staff. *17*
Personnel Authorized to Declare an Emergency *18*
Initial Assessment *18*
Incident Command Center *19*

Evacuation Procedures *20*
Guidelines: *21*
Key Contacts *22*
Incident Response Team: *22*
Employee: *22*
Corporate: *23*
Media: *23*
Suppliers and Vendors: *24*
Medical and Emergency: *24*
Generator: *25*
Facility Maintenance: *25*
Utilities: *26*
Communications *26*
Internal: *27*
External: *28*
Recovery Strategies *29*
Bibliography 32
References Cited in This Document *32*
Suggested Reading and Other Resources *32*
Appendix A: Pandemic Preparedness 33
Appendix B: Incident Response Manual 36
Appendix C: Model Radio Vulnerability Assessment Checklist 39
Appendix D: Incident Command Center Inventory Template 43
Appendix E: Emergency Evacuation Plan Template 45
Appendix F: Survey Form Template 53

List of Figures

Figure 1: Basic recovery planning steps 1

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..... 12
Table 5: Incident command center location..... 19
Table 6: Incident response team 22
Table 7: Employee contact information..... 22
Table 8: Corporate contact information..... 23
Table 9: Media contact information..... 23
Table 10: Suppliers and vendors..... 24
Table 11: Medical and emergency contacts..... 24
Table 12: Government Contacts…….26

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. **[Radio station]** is encouraged to adapt its use to accommodate any unique requirements which 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.

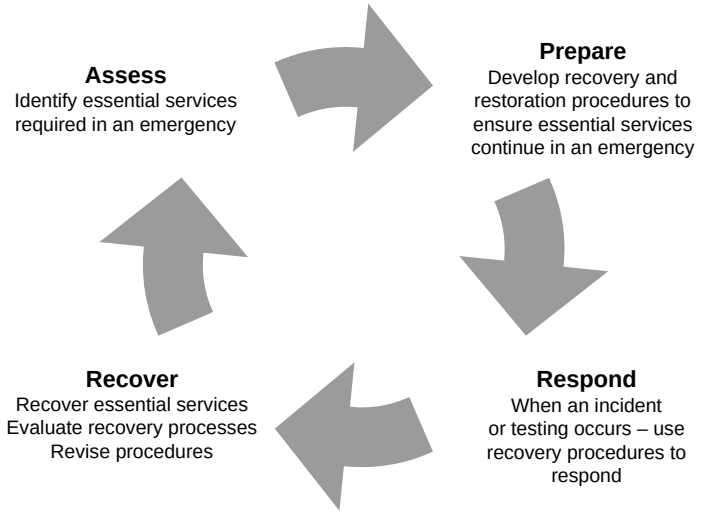

Figure 1: Basic recovery planning steps

The objective of this document is to provide guidelines and strategies that will allow [Radio station] 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.

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 eruption, earthquake 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 with the Incident Response Team.

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

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 routinely backed up.

- 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 and Network Operations Center (NOC) .

- 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 which 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 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, 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, audio processing chain, network operating software, changes to signal wire 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., Air Studio, Production Studio, News Room, Rack Room, STL origination, Digital audio (IBOC) or digital radio advanced data services Transmitter Site).

- Significant modification of business or operational support systems (i.e. traffic and billing systems, music scheduling systems, automation systems, 3rd party interfaces to external systems i.e. tagging, traffic or weather data services, textual emergency alerts or anything that integrates with and affects day to day technical operations).

- Personnel transfers, terminations, promotions, relocation (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 3rd 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 station Technology Manager (Title will vary depending on the company such as Chief Engineer, Director of Engineering) 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 Chief Engineer should meet to identify all critical components of the air chain 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. A test for loss of main air studio may involve switching to the news room or production studio, or may involve setting up the station's remote vehicle to provide on air material.

The input of all affected parties, such as DJ's, Talk Show hosts, traffic managers, digital content managers and others including non-technical personnel should be requested so that routine tasks essential to the normal operations of the radio station are not overlooked.

While conducting DRP testing, it is essential to carefully document events as they occur during the test, noting any unexpected, unusual or abnormal system 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 which 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 example, while conducting a test of the DRP for a complete evacuation of a facility such as 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 inter-operability 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 need to be customized for all locations.

Schedule of Plan Testing

It is required that a schedule be developed for testing of each critical system and subsystem. For example, the "loss of transmitter" test might be scheduled during the night to avoid drive time interruption of service. Critical systems should be tested more often than ancillary subsystems. The Disaster Recovery Planning Manager may require "loss of transmitter" testing every three months, while "loss of air studio" testing may be performed only once or twice per year and "loss of audio processing" less often. 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.

A local station that was testing its UPS and emergency power monthly, fully expected to pass their annual test with all the power fully disconnected from the utility power grid. All systems ran correctly as expected except that the main newsroom had no lights. The newsroom was completely dark. During a recent electrical renovation the newsroom lighting was connected to the wrong power source. This situation would not have been found without this type of test.

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 automation system is to be tested, technology support (Title will vary depending on the company such as Engineering, IT, etc) should make sure that all data 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 the stations on air program material (dead air).
In the event of a main transmitter systems test, steps must be taken in preparation for the backup transmitter to be on standby in case unforeseen events prevent the main transmitter from returning to or remaining on the air. In a typical radio engineering 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

In this section, all critical systems and subsystems are identified and categorized by order of priority for creating a DRP testing strategy. Each radio station may have its own particular vulnerabilities. As vulnerabilities are identified, a corresponding testing plan needs to be developed. Here are some examples:

- **Disaster -** Loss of transmitter site / tower, **Recovery –** Backup transmitter site.
- **Disaster** – Loss of Air Studio, **Recovery** – move operations to newsroom or production studio.
- **Disaster** – Evacuation of building, **Recovery** – move operations to remote studio vehicle or location.
- **Disaster –** Loss of critical system data – **Recovery –** initiate file recovery procedures

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 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 to 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 listeners' enjoyment of regularly scheduled programming?
- 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 and 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 a testing protocol is agreed upon by all concerned departments. Proper planning, testing and implementation of recovery strategies will facilitate a fast and complete return to "normal" operations during an emergency. Listeners will remember that it was your radio station that stayed on the air and relayed important news and critical emergency information during the crisis.

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 which potentially may exist in **[Radio station]**, a model Radio Broadcast 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 **[Radio station]** is encouraged to adapt its use to accommodate any unique requirements which 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 which potentially may exist. **[Radio station]** 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.

- While keeping all aural and data services on the air is most desirable, ensuring that the aural services remain on the air to serve the community is an absolute necessity. The focus of prevention considerations should be on facilities that have a role in originating or delivering news and/or emergency warnings and notices to the public.

- Disaster recovery plans should be periodically updated, tested and rehearsed.

- Some capability should exist to obtain news and information in an emergency situation such as an alternate studio, remote studio or an arrangement to receive signals from local television and/or cable broadcasters (e.g., ENG/SNG trucks or satellite links.)

- Backup radio and television receiver capabilities should exist for relaying breaking news and information. The use of DBS receivers is encouraged to provide news and information during regional widespread emergencies which may affect other local and regional broadcasters.

In March of 2000, a small brush fire caused the Four Corners Generating Station to trip off line resulting in a power outage affecting almost the entire state of New Mexico. While I was on my way to the main studio to start the main generator (fueled by natural gas and connected to the natural gas main for a virtually unlimited fuel supply in preparation for Y2K), I tuned across the radio dial and was met with an eerie silence as every broadcast station within receiver range was off the air. This included FM, AM and Television stations originating in Albuquerque 130 miles distant! The KTAO radio station transmitter is entirely solar powered and within 15 minutes after the outage began, KTAO was back on the air at full power and for about an hour was the only station in North Central New Mexico that was fully operational. This power outage affected a very large area and was caused by a relatively small brush fire under a power line.

- When completing the Vulnerability Assessment Checklist it is prudent to consider the location and geographic distribution of key facilities in the market, advances in mobile or non-mobile broadband Internet near your facilities such as studios, STL origination sites, transmitter sites and translator locations.

- Appropriate measures should be taken to provide redundant, geographically diverse methods and equipment for delivering program material to the STL, Internet-based connectivity, transmitter, backup transmitter and translator sites.

- Collaboration with other local broadcasters should take place to increase collective site and equipment diversity, redundancy and interconnections. In times of emergency, "share the wealth" to ensure that all segments of the community are well served.

- Appropriate measures should be taken to "harden" the broadcast facilities, studios and transmitter sites, particularly in areas prone to severe weather or natural disasters.

- Appropriate measures should be taken to provide backup power capabilities for all key facilities, including main studios, STL origination sites, transmitter and translator sites.

- Essential equipment and service suppliers should be examined to ensure that critical resources will have sufficient capacity and delivery capabilities to meet needs during an emergency. This is particularly important where fuel for backup generators is concerned. **[Radio station]** should consider securing arrangements for fuel deliveries from suppliers located outside of the local market during emergency situations.

- Physical security such as chain link fences augmented by security personnel and/or video surveillance is recommended at all sites critical to the broadcast operation.

- Radio broadcasters should have appropriate physical security, augmented by security personnel and/or video surveillance at their key facilities, including studios/newsrooms, satellite transmit and receive sites and antenna/transmitter sites.

- Radio Broadcasters should employ diverse power grid sources wherever feasible.

- Radio broadcasters should take appropriate measures to provide backup power capabilities for their key facilities, including studios/newsrooms, satellite communications and transmitters.

- Radio broadcasters with local news origination should ensure that they have robust and redundant ways to communicate with external news services and remote news teams, such as the use of mobile radio and Internet to augment cell phones.

- Radio broadcasters should have backup signal feeds to their primary satellite transmit and receive sites.

- Radio broadcasters should have redundant signal paths to their primary and backup transmission facilities.

- Radio broadcasters with local news origination should plan to have emergency origination capability at a separate location from their primary studio (e.g., backup studio, transmitter site, remote van, another station, etc).

- Radio broadcasters should plan IT disaster recovery procedures for sourcing replacement infrastructure (routers, switches, firewalls), servers, computers and software media needed to restore operate the facility or operation. Data services for communication such as email, Internet access and critical data files should be coordinated with IT recovery procedures.

- Radio broadcasters with local news origination should have a remote vehicle, or some means of delivering live news and information from a remote site.

- Radio broadcasters should have the capability of receiving a remote feed at an additional site from their primary studio (e.g., directly at their tower site, at a backup studio, etc).

- Radio broadcasters should have a backup satellite transmitter and receiver, or an alternate means (e.g., a Satellite Radio receiver, a dedicated phone line or a streaming audio Internet connection) to send and receive signals from and to national news services in emergency situations.

- Radio broadcasters should have a backup transmitter, and should attempt to make practical arrangements for geographic diversity where possible (e.g., provisions for emergency use of other backup transmitter/antenna facilities in the community or other means).

- With the cooperation of federal and local policy makers, all radio broadcasters in a market should collaborate to increase their collective site diversity and redundancy, including news studios; operations; satellite transmit/receive facilities and transmitter/ antenna sites.

- **[Radio station]** 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.

- **[Radio station]** 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.

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 **[Radio station]** 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 **[Radio station]** personnel.
- Coordinate communications with essential equipment and service suppliers, including contract engineers, 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 key 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 **[Radio station]** 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 that primary and alternate facilities are secure.
- Ensure adequate and secure long-term parking for personnel.
- Coordinate communications with **[Radio station]** 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 **[Radio station]** DRP can be updated, tested and implemented as specified.
- Ensure that personnel are familiar with the **[Radio station]** DRP.
- Ensure that there are reciprocal agreements with other local broadcasters and cable operators.

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 bases 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 **[Radio station]** operations and delivery of essential services. An emergency event may not require that the entire DRP be implemented. Each event should be evaluated on its impact and severity by the Incident Response Team and Management.

Initial Assessment

These general guidelines should be followed by the individual(s) discovering or responding to the emergency situation. If possible and time permits, the following assessment process should occur:

- Assess the situation. Consider your safety as 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.

  - 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 offices.

  - 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 entire plan be implemented. Each event should be evaluated on its impact and severity by the Incident Response Team, Disaster Recovery Planning Manager or Management.

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

Primary Locations	Address	Contact
Secondary Locations	**Address**	**Contact**

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. **[Radio station]** 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 will be needed for the next 48-72 hours?

Evacuation Procedures

This section is designed to assist **[Radio station]** 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 **[Radio station]** is provided in Appendix D.

During the Hurricane Katrina recovery at WQRZ-LP in Bay St. Louis, MS during September 2005, a situation occurred while Hurricane Rita was affecting the already devastated area. WQRZ-LP was co-located with the Hancock County Emergency Operations Center. While WQRZ-LP was receiving a Tornado Warning on the EAS, a fire alarm was activated in the building because of a faulty air handler motor. Fire Safety personnel were attempting to evacuate *essential* radio station personnel while the announcer was broadcasting a Tornado Warning which included the Hancock County EOC in the path of the Tornado. This is an example of conflict of authority and responsibility and situations such as this should be addressed in the planning phase of the Evacuation Process.

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 Security, EHS, On Air, Distribution, Production, Corporate Communication, Legal, , Network Operations Center (NOC), information technology (IT)Human Resources, Medical, Facilities, Sourcing and Finance as applicable.

- 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 a predetermined basis after evacuation occurs.

- Develop a training program for distribution and review by personnel.

- Coordinate the EEP with the **[Radio station]** 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 and 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 delivery 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
		Office: **Home:** **Cell:**	

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

[Radio station] 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 **[Radio station]** 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 **[Radio station]** 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 a disaster or other emergency situation. **[Radio station]** should consider creating e-mail distribution lists so that e-mail messages are broadcast to all members on 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 when ever this type of resource will be utilized and directed to the one that will be used to provide information about **[Radio station]**.

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, **[Radio station]** 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, municipalities, federal agencies (e.g., FCC, FEMA, etc.), elected officials, opinion leaders, customers, and suppliers.

During and after emergencies, these external entities may frequently contact **[Radio station]**. These contacts may be general inquiries, requests for sensitive information, requests for assistance, or they 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. **[Radio station]** may also wish to consider activating emergency alert systems. The Federal Communications Commission encourages broadcast licensees to transmit emergency alerts as a public service.

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

Recovery Strategies

All recovery plans should start with an assessment of the vulnerabilities within **[Radio station]**. It is the responsibility of the Disaster Recovery Planning Manger to work with **[Radio station]** 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 (*Disaster Recovery 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 back on the air 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 which may not be initially apparent.

There are nearly an infinite number of natural or man-made disasters or other emergency situations which could occur including bomb threats, earthquake, fire, flooding, gas leak, 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 **[Radio station]** could potentially encounter due to an emergency situation include:

- Station On-the-Air / Off-the-Air.
- Loss of the transmitter building.
- Loss of master control or STL.
- Lock down - personnel cannot leave the facilities.
- Mandatory evacuations.
- Personnel cannot access the facilities or into the building(s).
- Transmitter tower issues.
- Loss of telephony wired/wireless.
- Loss of data networking capabilities.
- Loss of communications capabilities to field personnel.
- Newsroom computer system failures.
- Satellite distribution system 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. **[Radio station]** 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 snow storms is not.

Example: Loss of power at the studio

Recovery Strategy	Preparation Considerations	Responsibility	Procedures
Start the emergency generator and transfer the building load to it.	Proper maintenance on the generator. Proper testing of the generator. Sufficient fuel. Source of fuel during extended operation.	*[Outline each area of responsibility and have qualified staff to accomplish the tasks necessary]*	Any special procedures needed for the recovery.

Example: Evacuation of main studio/master control

Recovery Strategy	Preparation Considerations	Responsibility	Procedures
Switch to backup studio site; Set up RPU for direct connection to the transmitter.	Design a system to enable remote connection of RPU and/or backup studio directly to the transmitter. Test remote control of program source switching under realistic conditions.	*[Outline each area of responsibility and have qualified staff to accomplish the tasks necessary]*	Staff communications and evacuation plan, a place for the staff to meet external to the facility.

Bibliography

References Cited in This Document

Media Security and Reliability Council. (2005, September 19). *Local radio station model vulnerability assessment checklist*. Retrieved September 19, 2005 from http://www.mediasecurity.org/documents/ RadioVulnerabilityChecklist.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

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

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 Reliability and Interoperability Council, http://www.nric.org

Toigo, J. (2003). *Disaster recovery planning: Preparing for the unthinkable (3rd 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 which 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., immuno-compromised 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
(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
(Occupational Safety and Health Administration website)

www.cdc.gov/niosh
(National Institute for Occupational Safety and Health website)

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 **[Radio station]** DRP in various locations and sections are duplicated here. It is intended that the Incident Response Manual be carried by team members at all times. 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

Primary Locations	Address	Contact
Secondary Locations	**Address**	**Contact**

Employee Contact Information

Table 3: Employee contact information

Name	Title	Contact	Responsibilities
		Office: **Home:** **Cell:**	

Selected Suppliers and Vendors:

Table 4: Selected suppliers and vendors

Company Information	Representative	Contact
		Office: **Home:** **Cell:**

Medical and Emergency:

Table 5: Medical and emergency contacts

Company	Address	Contact
		Office: **Home:** **Cell:**

Appendix C: Model Radio Vulnerability Assessment Checklist

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

Disaster Recovery Plan		
Does a Disaster Recovery Plan exist which details how to effectively assess impact to the facilities and recovery operations in the event of an emergency?	☐ Yes	☐ No
Does the Disaster Recovery Plan address timely activation of any backup origination facility in time of emergency?	☐ Yes	☐ No
Does the Disaster Recovery Plan include backup delivery methods for network or other programming?	☐ Yes	☐ No
Does the Disaster Recovery Plan include reception and delivery of emergency news?	☐ Yes	☐ No
Does the Disaster Recovery Plan identify essential personnel necessary to carry out restoration efforts?	☐ Yes	☐ No
Does the Disaster Recovery Plan include agreements to gain assistance from other broadcast, cable and production operations?	☐ Yes	☐ 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?	☐ Yes	☐ 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?	☐ Yes	☐ 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)?	☐ Yes	☐ No

Is the Disaster Recovery Plan periodically reviewed and updated?	☐ Yes	☐ No
Is the Disaster Recovery Plan periodically tested and rehearsed?	☐ Yes	☐ No

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

Studio Planning			
Backup Origination Facilities	Does a backup studio exist at an offsite location?	☐ Yes	☐ No
Backup Power	Does the Studio facility have backup power?	☐ Yes	☐ No
	Does the primary transmission facility have backup power?	☐ Yes	☐ No
	Does the backup studio facility have backup power?	☐ Yes	☐ No
	Does the backup transmission facility have backup power?	☐ Yes	☐ No
	Can backup power operate long enough to implement the recovery plan?	☐ Yes	☐ No
	Where backup power is available is it automatically activated?	☐ Yes	☐ No
	Are the backup power systems routinely tested under load?	☐ Yes	☐ No
	At least once a year is the backup power tested while the facility is disconnected from the power grid?	☐ Yes	☐ No
Security	Are security protocols sufficient to prevent unauthorized access to the studio facilities?	☐ Yes	☐ No
Emergency News & Information	If national network news agreements do not exist, is there an agreement to carry emergency news from alternate sources?	☐ Yes	☐ No
	In the event of a failure of the newsroom computer system is there an alternate plan	☐ Yes	☐ No

Studio Planning			
	to get news on the air?		
	Can Emergency Alert System ("EAS") alerts be received and rebroadcast from backup facilities, if such facilities exist?	☐ Yes	☐ No

Terrestrial Transmission			
Backup Transmission Facilities	Is there a backup transmitter and antenna available?	☐ Yes	☐ No
	If there is a backup transmitter and antenna site, is it geographically diverse from the primary location?	☐ Yes	☐ No
	Does the backup transmitter and antenna provide service to the metro area?	☐ Yes	☐ No
Backup Power	Does the primary transmission facility have backup power?	☐ Yes	☐ No
	Does the backup transmission facility have backup power?	☐ Yes	☐ No
	Can backup power operate long enough to implement the recovery plan?	☐ Yes	☐ No
	Where backup power is available is it automatically activated?	☐ Yes	☐ No
	Are the backup power systems routinely tested under load?	☐ Yes	☐ No
	At least once a year is the backup power tested while the facility is disconnected from the power grid?	☐ Yes	☐ No
Security	Are the security protocols sufficient to prevent unauthorized access to the transmission facilities?	☐ Yes	☐ No
Redundant Signal Routes	Is there a backup signal path to the primary transmitter facility?	☐ Yes	☐ No
	Do these redundant paths include diverse technologies, (i.e., wired and wireless)?	☐ Yes	☐ No
	Is there a backup signal path to the backup transmitter facility?	☐ Yes	☐ No

	Do these redundant paths include diverse technologies, (i.e., wired and wireless)?	☐ Yes	☐ No
	Are there auxiliary TV or radio tuners at the transmitter site that can be used as an alternate source of news and information?	☐ Yes	☐ No
	Is a RPU system available for remote broadcasts?	☐ Yes	☐ No
	Can the RPU signal be received at the transmitter site?	☐ Yes	☐ No
	If so, can the RPU signal be switched into the transmitter by remote control?	☐ Yes	☐ No
Transmission remote control	Can the transmitter site(s) be remotely controlled from locations other than the main studio?	☐ Yes	☐ No
	Can the transmitter site(s) be controlled with diverse technologies, (i.e., wired and wireless)?	☐ Yes	☐ No
Business Systems			
	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?	□ Yes	□ No

Appendix D: Incident Command Center Inventory Template

Category	Item	Quantity	Location
Food	Cook stove/fuel		
	Paper towels		
	Aluminum foil		
	Plastic wrap		
	Paper plates		
	Forks/spoons/knives		
	Cooler		
Water	Drinking		
	Washing		
Lighting	Flashlights		
	Batteries		
Radio/TV	Radios (battery)		
	Batteries		
	TV (battery)		
	Batteries		
Facilities	Beds		
	Bedding		
	Towels		
	Personal hygiene		
	First aid kit		
Data Network	PC		
	Laptop		
	Wireless router		
	Ethernet switch		
	Broadband access		
	Dial-up modem		
	Dial-up access		
Voice Network	Cellular phones		
	Analog/fax lines		
Documentation	DRP/IRM	2 copies	
	Facility	2 copies	
	Network		
Tools	Basic hand tools		

Category	Item	Quantity	Location
	Hardhat		
	Coveralls		
	Duct tape		
	Shop vacuum (wet/dry)		
	Broom		
	Dust pan		
	Gloves		
	Rubber boots		
	Safety glasses		
	Fire Extinguisher		
	Sheet plastic		
Office Supplies	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 **[Radio station]** such as fire, explosion, hazardous material spill, 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 which clearly show the emergency escape routes included in the EEP. Color-coding 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 **[Radio station]** 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 fire box 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 Transition	Name	Contact
			Office: **Home:** **Cell:**

The shutdown procedure to be followed by those employees who have been assigned to care for essential **[Radio station]** 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 to 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 **[Radio station]** appears in Table 2.

Table 2: EEP Contact information

Responsibility	Name	Location	Contact
Emergency Evacuation Coordinator			**Office:** **Home:** **Cell:**
Alternate Emergency Evacuation Coordinator			
Safety Monitor			
Alternate Safety Monitor			

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.

Training attendance records should be maintained by the Emergency Evacuation Coordinator and/or Disaster Recovery Planning Manager.

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

Call Sign: _____ City of License: _____

Market: _____ Owner: _____

Other Stations in Market: _____

Headquarters Contact Person (out-of-area): _____
Title: _____
Phone Number: _____ Cell: _____
Email: _____

Data/Needs Contact Person (local):_____ Title: _____
Phone Number: _____ Cell: _____
Email: _____

Studio Address: _____
Studio backup generator: _____
Fuel type and capacity: _____
Backup studio facilities: _____
Location: _____

Transmitter Site Address: _____
Transmitter Site Contact Person: _____
Phone Number: _____ Cell: _____

Transmitter site backup generator? ___Yes ___No
Fuel type and capacity: _____
Will operate stations how long? ___hours ___Days
Station power/ERP with Generator: _____

How does station get signal to transmitter site? _____

Date off air: _____
Date resumed with generator: _____
Date station resumed operations with commercial power:_____