**Incident Management Plan Template**

**By: FieldPoint Service Applications Inc.**

*Revision 0.0*

*Date: June 26, 2013*

**Revision History**

|  |  |  |
| --- | --- | --- |
| **Revision date** | **Items revised** | **Author** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**Table of Contents**

1.1 Introduction 3

1.2 Incident response plan overview 3

1.3 Scope 4

1.4 Exclusions 4

1.5 Examples of Planning Scenarios 4

1.5.1 Loss of data communications, e.g., WAN, routers 4

1.5.2 Loss of technology, e.g., computer room, network services 5

1.5.3 Loss of people, e.g., illness, death 5

1.6 Recovery objectives 5

1.7 Assumptions 6

2.1 Logical Sequence of Events 6

2.2 Incident Management Team 7

Personnel Contact List 8

## Introduction

**General information**

This manual was developed for “BUSINESS NAME”. Due to the sensitive nature of the information contained herein, this manual is available only to those persons who have been designated as members of one or more incident management teams, or who otherwise play a direct role in the incident response and recovery processes.

The following teams will appear throughout this plan:

* NETWORK OPERATIONS CENTER
* INCIDENT PERSONNEL
* DAMAGE ASSESSMENT TEAM
* TEAM LEADS AND MANAGEMENT

## 1.2 Incident response plan overview

**Overview and objectives**

This incident management plan establishes the recommended organization, actions, and procedures needed to

* Recognize and respond to an incident;
* Assess the situation quickly and effectively;
* Notify the appropriate individuals and organizations about the incident;
* Organize the company’s response activities, including activating a command center;
* Escalate the company’s response efforts based on the severity of the incident; and
* Support the business recovery efforts being made in the aftermath of the incident.

This plan is designed to minimize operational and financial impacts of such a disaster, and will be activated when a local Incident Manager (or, in his/her absence, one of his/her alternates) determines that a disaster has occurred.

#

## 1.3 Scope

This incident management plan includes initial actions and procedures to respond to events that could impact critical business activities at BUSINESS NAME AND LOCATION. This plan is designed to minimize the operational and financial impacts of disasters.

##

## 1.4 Exclusions

This plan specifically excludes the following from its scope:

* Facilities not located at the BUSINESS NAME AND LOCATION

##

## Examples of Planning Scenarios

This plan was developed to respond to incident scenarios such as the following:

1. Loss of data communications and the network infrastructure
2. Loss of technology
3. Loss of professional staff (e.g., via a flu outbreak)

### *1.5.1 Loss of data communications, e.g., WAN, routers*

Any incident that disables or destroys the WAN router infrastructure and its communication capabilities located at BUSINESS NAME AND LOCATION, with a potentially disruptive effect on business operations.

This scenario could produce one or more of the following impacts:

* Loss of access to the WAN
* Loss of access to the Internet and intranet
* Incident is declared and incident recovery actions are implemented
* Use of recovery strategies, commercial hot site, reciprocal agreements, and manual operations as a temporary measure
* Business shutdown
* Need for new facilities/equipment

### *1.5.2 Loss of technology, e.g., computer room, network services*

Any incident that disables or destroys the entire computer room facility or its processing capacity located at BUSINESS NAME AND LOCATION, with a potentially disruptive effect on business operations.

This scenario could produce one or more of the following impacts:

* Loss of use of the computer room facility
* Loss of voice/data communications services
* Incident is declared and incident recovery actions are implemented
* Use of recovery strategies, commercial hot site, reciprocal agreements, and manual operations as a temporary measure
* Business shutdown
* Need for new facilities/equipment

##

### *1.5.3 Loss of people, e.g., illness, death*

Any incident that disables or renders the professional staff at BUSINESS NAME AND LOCATION unable to perform normal business functions, with a commensurate negative effect on business operations.

This scenario could produce one or more of the following impacts:

* No impact to building access or technology infrastructure
* Insufficient professional staff to perform minimal business operations
* Lack of suitably cross-trained staff
* Business shutdown
* Need for temporary staff

## 1.6 Recovery objectives

This incident management plan has been developed to meet the following objectives:

1. Provide an organized and consolidated approach to managing initial response and recovery activities following an unplanned incident or business interruption, avoiding confusion and reducing exposure to error.
2. Provide prompt and appropriate response to unplanned incidents, thereby reducing the impacts resulting from short-term business interruptions.
3. Notify appropriate management, operational staff and their families, customers, and public sector organizations of the incident.
4. Recover essential business operations in a timely manner, increasing the ability of the company to recover from a damaging loss at LOCATION.

## 1.7 Assumptions

This plan has been developed and is to be maintained on the basis of the following assumptions:

* Add List of Assumptions

## 2.1 Logical Sequence of Events

**EXAMPLE OF INITIAL INCIDENT RESPONSE CHECKLIST**

|  |  |
| --- | --- |
| COMMAND CENTER - CREATES INCIDENT TICKET | [ ]  |
| DISPATCH PROCEDURES - RESOURCE ALLOCATION AND SCHEDULING  | [ ]  |
| NOTIFICATIONS OF ASSIGNMENTS AND WORK ORDERS | [ ]  |
| TEAM REJECTS OR ACCEPTS ASSIGNMENT(S)  | [ ]  |
| WORK ORDER DETAILS SENT: TIME, LOCATION, TASKS, ETC.  | [ ]  |
| ASSIGNED PERSONNEL COMPLETED WORK ORDER  | [ ]  |
| COMPLETED WORK ORDERS ROUTED TO MANAGERS FOR APPROVAL OR REJECT  | [ ]  |
| CLOSE OR RE-OPEN INCIDENT  | [ ]  |

##

## 2.2 Incident Management Team

A successful recovery can only occur with total coordination of all incident management and recovery activities. Teams have defined roles and responsibilities that contribute to the success of the recovery. INSERT TEAM DIAGRAM



|  |  |  |
| --- | --- | --- |
| **Name of Personnel** | **Role**  | **Responsibility** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

 **Roles and Responsibilities:**

## Personnel Contact List

|  |
| --- |
| **Incident Management Team** |
| **Last name** | **First name** | **Title** | **Department/Location** | **Work phone** | **Home phone** | **Alternate phone** | **Pager/Cell phone** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |