

## Disaster Recovery/Business Resumption Plan



**The City of Hillsboro, Ohio**

**Disaster Recovery/Business Resumption Plan  
City of Hillsboro, Ohio**

**Administrative Summary**

**Purpose**

The primary reason the City of Hillsboro is engaging in disaster recovery and business resumption planning is to ensure the ability of the organization to function effectively in the event of a severe disruption to normal operations. Severe disruptions can arise in several ways including natural disasters (lightning, tornadoes, fire, etc.), equipment failures, process failures, or even from malicious acts (such as network intrusion, viruses, and other invasive attacks).

While we may not be able to prevent any of these from occurring, planning for the worst enables the organization to resume essential operations more rapidly than if no plan existed. With disaster recovery planning, we are focusing on the set of actions we must take to restore service and operations in the event that a significant loss has occurred.

Our plan does not strictly focus efforts and planning on each type disaster but it looks to plan for commonalities between the outcomes of the disaster such as a loss of information, loss of personnel, loss of equipment, loss of access to information and facilities. Our plan will specify the set of actions to be performed for each activity in the event of any of these disruptions occur in order for the organization to resume doing business in a minimal amount of time.

**Scope**

The scope of work will be broken down into the following Phases:

- a) **Pre-Planning, Project Initialization Document (PID)** – This phase will create an approval process for executing this program. In this phase, an estimate of resources and impact to the business operations will be presented to City administration.
- b) **Detailed Definition of Requirements** – This phase will examine ways in which we can reduce the possibility of disaster occurring as well as performing a detailed assessment of security and associated risks.

- c) **Business Impact Assessment Phase** – This phase will examine all systems, processes and business functions within the organization. From these areas, an impact analysis will be performed on loss of these areas for set periods of times.
- d) **Detailed Definition of Requirements / Planning**– This phase will create the recovery strategy based upon severity of business impact risk. This plan will identify the critical resources, systems and services needed to support the areas of high business impact.
- e) **Test Plan Phase** – Testing goals will be created here in line with the above requirements. Strategies shall be created which are in line with the environment and service needs.
- f) **Maintenance Program Phase** – This phase will create a process in which the overall business continuity / disaster recovery program is kept current and maintained as government operations change the way we work.
- g) **Actual Testing and Implementation Phase** – The final step will be the actual testing of the business recovery programs. In this phase, execution of plans will occur, results documented and modified as needed.

## **Goals**

There are three goals for this Disaster Recovery Plan:

1. Limit or reduce the potential for injuries or loss of human life, any damage to the facility, or loss of records and assets. Steps to take:
  - Lower any type of disruptions that may adversely influence City services
  - Lower financial losses if any.
  - Operations back online in a timely manner
  - Limit liability against any claims that are filed
2. Take immediate steps to put our plan into effect and beginning the recovery process.
3. Implement the procedures in the plan and prioritize our efforts as such:
  - Employees: people come first they are our first concern in a time of emergency.
  - Customers: be sure to make a customer comfortable with what we are doing to be ready for any inconvenience

- Facilities: Secure the facility.
- Assets: conduct an assessment and decides what resources we have and which ones are still at risk.
- Records: Document everything that happens and videotape the proceedings for protection from liability.

### **Objectives**

Our primary objective is to maintain, resume, and recover key business resources once an interruption of business functions has occurred. The business continuity plan does not focus entirely upon technical resources, but will also consider the underlying business processes affected by government disruption due to disaster and system failure.

The business continuity plan shall consider each of the following areas:

- Business Impact Analysis
- Risk Assessment
- Risk Management
- Risk Monitoring

The plan emphasizes the organizational business processes as well as technology resources in the event of disruption and will endeavor to regain these business processes in a timely manner in order to minimize financial loss to the organization.

Upon finalization, the business continuity plan will be updated on a quarterly schedule, making the appropriate changes necessary to ensure a sound disaster recovery plan. The business continuity planning team shall be charged with the maintenance and testing of this plan.

### **Organizational Overview**

The organizational goals of the City of Hillsboro are to provide quality services to our constituents. Emergency calls for service and maintaining key public utilities services is our primary goal. The City will endeavor to maintain critical services in the event of disaster.

The City of Hillsboro maintains full-time police and fire services to a population of approximately six-thousand residents. Aside from our public safety services, the City also maintains a full-service public utilities department – providing sanitary water and sewer services.

The major business functions are:

- Police Service
- Fire Service
- Water Treatment
- Sewer Treatment
- Street Maintenance
- Structured Municipal Government

The mission of the City of Hillsboro's System Administrator is to support government business objectives by providing timely access to computing and telecommunications services, and to provide leadership in the use of information technology. In a disaster situation, its mission is to support the government disaster recovery.

### **Risk and Security Assessments**

#### **Risks**

The City of Hillsboro government entities are located throughout the City.

#### **Risks to Government Assets**

After conducting an in-depth business impact analysis, the following is a list of the most likely risks to government assets, they are:

- **Tornado**

Tornadoes are tight columns of circling air creating a funnel shape. The wind forces within the tornado can reach over 200 miles per hour. Tornadoes can often travel in excess of 50 miles per hour. They can cause significant structural damage and can also cause severe injuries and death.

- **Hurricane**

Hurricanes are storms with heavy circular winds exceeding 60 miles per hour. The eye or centre of the hurricane is usually calm. The hurricane contains both extremely strong winds and torrential rain. Hurricanes can cause flooding, massive structural damage to homes and business premises with associated power failures, and even injury and death.

- **Flood**

Floods result from thunderstorms, tropical storms, snow thaws or heavy and prolonged rainfall causing rivers to overflow their banks and flood the surrounding areas. Floods can seriously affect buildings and equipment causing power failures and loss of facilities and can even result in injury or death.

- **Snowstorm**

Snowstorm conditions can include blizzards, strong winds, freezing temperatures with significant amounts of snow. Snow and ice can impact power and communications and employees may be unable to travel to work due to the impact on public transport or road conditions. It is possible for buildings to collapse under the weight of snow and injuries or even death could occur through freezing temperatures and icy conditions.

- **Drought**

Droughts are caused through lack of rainfall and can have a devastating affect on human life, animal life and plant life. These conditions are often seasonal and some regions of the world are more prone to these extreme conditions. Severe droughts can cause considerable loss and suffering to human life. There can also be significant affects on businesses that depend on the availability of water for their products or processes.

- **Earthquake**

Earthquakes are caused by a shifting of the earth's rock plates beneath its surface resulting in violent shaking and movement of the earth's upper surface. Severe earthquakes can destroy power and communication lines and disrupt gas, water and sewerage services. Significant damage to structures can occur including total collapse of buildings, bridges or other elevated structures. Earthquakes can also bring landslides, damage to dams, and aftershocks and resulting damage can hinder rescue efforts. In addition to being trapped in a collapsing building, of particular danger to human life is the possibility of falling glass or other objects.

- **Electrical storms**

The impact of lightning strikes can be significant. It can cause disruption to power and can also cause fires. It may also damage electrical equipment including computer systems. Structural damage is also possible through falling trees or other objects.

- **Fire**

Fires are often devastating and can be started through a wide range of events which may be accidental or environmental. Deliberate fires caused through arson are dealt with in topic BC 020102. The impact on the business will vary depending on the severity of the fire and the speed within which it can be brought under control. A fire can cause human injury or death and damage can also be caused to records and equipment and the fabric or structure of premises.

- **Subsidence and Landslides**

Subsidence and landslides are often caused through a change in the composition of the earth's surface. This change can often result from flooding, where flowing water can create cavernous open areas beneath structures. Subsidence or landslides can cause structural damage and can also disrupt transport services and affect traveling conditions.

- **Freezing Conditions**

Freezing conditions can occur in winter periods and the effects can be devastating. Where temperatures fall in excess of - 30(Centigrade they can create conditions which significantly disrupt businesses and even cause death or injury. Businesses and homes can be seriously affected through burst pipes, inadequate heating facilities, disruption to transportation and malfunctioning equipment. Work undertaken outside of buildings in the open environment will obviously be seriously affected.

- **Contamination and Environmental Hazards**

Contamination and environmental hazards include polluted air, polluted water, chemicals, radiation, asbestos, smoke, dampness and mildew, toxic waste and oil pollution. Many of these conditions can disrupt business processes directly and, in addition, cause sickness among employees. This can result in prosecution or litigation if more permanent damage to employees' health occurs.

- **Epidemic**

An epidemic can occur when a contagious illness affects a large number of persons within a country or region. This can have a particularly devastating short term impact on business through a large number of persons being absent from work at the same time. Certain illnesses can have a longer term effect on the business where long term illness or death results. An example of this extreme situation is occurring in certain third world countries where the Aids virus is considered to be of epidemic proportions.

Many different scenarios may be identified as disasters; from the loss of a single file server, to the total devastation of a government facility.

In the event of government Information Systems disruption, the City of Hillsboro must take all appropriate measures to regain functionality in key business areas. Given the location of business resources, the most likely risk to government resources are: power disruptions, fire, natural disaster, employee actions, and acts of terrorism. Aside from the catastrophic physical impact of the previously noted risks, the City of Hillsboro also considers the possibility of computer network intrusion and computer viruses as a potential external threat to government resources.

Chief among the potential risks to government resources is the threat of employee actions, both intentional and accidental. The primary risks associated with employee use of government network resources are: "instant messaging, peer-to-peer applications, spyware and malicious mobile code, employee hacking, and streaming media." A common flaw in assessing government risks is the emphasis upon outside risks. It is important to note that "there are significant emerging threats to security that are not being introduced from external, unknown sources, but from employees themselves. It's critical that organizations acknowledge these 'inside-out' risks."

### **Security Risks**

Security risks come in many forms. The major security areas identified are the following: Employee Sabotage, External Attacks / Virus Threats and Content Management. These areas are detailed below.

- Employee sabotage is the highest priority of concern and risk to the organization. Statistically over 80% of security breaches are caused by insiders - most often employees.
- More than 20% of attacks on government WEB sites are coming from the inside!
- Almost 30% of companies experience more than five attacks from the inside per year

Another security risk identified during the initial assessment involves external hacking, virus attack and the resulting damage. The City of Hillsboro has implemented robust user access tools as well as user level monitoring via our firewall(s). The City of Hillsboro also maintains a robust virus scanning process on all incoming traffic and attachments; to date we have not experienced any monetary loss associated with such an attack. Current impact estimates are minimal with our current control processes in place. In the area of security, the resources needed to respond and control any breach have been identified within the organization.

### **Organization of Disaster Response and Recovery Team**

#### **Administrative Steering Team**

Prior to any disaster occurring, the Administrative Steering Team will establish a clear set of roles and responsibilities for all groups within the organization, as they relate to disaster response. It is this team that will establish the chain of command the organization will follow in the disaster emergency. They will be accountable for not only setting up the proper management teams, but to approve all processes which will be followed as well. The members of the Administrative Steering Team are as follows:

- a) The Mayor
- b) The Safety/Service Director
- c) Police and Fire Chiefs
- d) City Law Director

This administrative team will establish the disaster management and response groups, which will be activated in the case of an actual disaster. These core response groups are as follows:

- a) The Business Continuity Management Team
- b) The Service Area Recovery Team(s)

### **Business Continuity Management Team**

The business continuity management team is the overall response and coordinating team in the case of a disaster. In such an event, this will be the governing body for all decisions, communications and response. This team will not only guide the City through the life of the disaster, but they will also create and empower the Functional Area Recovery Teams (s) as needed.

The core members of this Business Continuity Management Team are as follows:

**Safety/Service Director:** The chair of the team, this person is responsible for the overall functionality and operations of the Management Team.

**Police Captain:** Department Head over all police services

**Asst. Fire Chief:** Department Head over all fire and rescue services.

**Dept. Head Street Department:** Department Head over all public access related issues

**Dept. Head Water/Sewer Maintenance:** Department head over the restoration of water and sewer service.

### **Functional Area Recovery Team(s)**

In the event of an actual disaster, the immediate function of the Business Continuity Management Team will be to meet and appoint the required Disaster Response and Recovery Team(s). It will be these "on the ground" teams that actually respond to the disaster, correct as appropriate and report back to the Business Continuity Management Team status and actions.

As each disaster is unique, there will be no set formation to these groups, but core roles will need to be established for each. These are as follows:

- a) **Team Leader** – The overall supervisor for the response team. This role will be assigned as to availability and required skill set for the situation. This role is critical to the overall success of the team. This role will own the assignment of all people into his/her response team.
- b) **Communication Lead** – This role owns the overall internal and external communications surrounding the disaster and the response. This role will be the only interface to outside news agencies, internal communications or written documentation.

- c) **IT Lead** – This is the lead role over all system, network and application areas. This also includes assigning the telecommunication role as needed.
- d) **HR Lead** – As all events will impact people to some extent, this role will be responsible for all people related issues and events.

### **Disaster Response**

In the event of a disaster, the following steps will be taken as the immediate response:

- 1) Business Management Continuity Team Emergency Meeting – All available members of this team will respond to an emergency meeting in which the following steps will be taken.
  - i. Establish initial Response Team and Leader
  - ii. Initiate initial damage assessment estimate.
  - iii. Communicate initial message to administrative leadership team.
- 2) The Initial Response Team shall engage a damage assessment and review around the overall disaster. This assessment shall be conducted as follows:
  - i. Must be completed within 2-4 Hours.
  - ii. Must provide communication back to Business Management Continuity Team
  - iii. Must include recommendations on course of action.
- 3) Business Management Continuity Team meets to review the assessment and to execute the following:
  - i. Formal creation of all needed response teams.
  - ii. Formal assignment of all critical roles into response teams.
  - iii. Formal communication to Administrative Leadership Team on Disaster and Response.
  - iv. Commencement of Disaster Recovery Program
- 4) Response Team(s) respond and complete the overall Disaster Recovery Program.
  - i. IT Systems and Networks established
  - ii. Business Operations Restored

- iii. Health and Human Safety Issues Corrected
  - iv. Internal and External Communications Controlled
  - v. Communications Provided to Business Continuity Management Team as well as Administrative Leadership Team.
  - vi. Post-Mortem of disaster response to determine the following
    - 1. Cause of Disaster
    - 2. Response Effectiveness
    - 3. Documentation of Issues and Actions.
- 5) Business Continuity Management Team – Final Meeting
- i. Review Response Team Results
  - ii. Review Actions and Recommendations
  - iii. Disband Response Teams when Disaster Recovered

### **Disaster Notification and Formal Communication of Response Plans**

From the above response plan, it is evident that the core response and recovery processes revolve around a formal process of notification and communication control. These areas are critical for the proper disaster response and the engagement of the teams. Also, the need for control on communications is critical during a time of emergency, for the sake of impacted employees, constituents and overall government operations.

The following communication and notification principles will be followed in all phases of the disaster response:

- 1) **Common Source** – All information needs to come from a central source within the organization. This source needs to be aligned to the actual disaster, the impact on the organization and community and the overall communication plan. This source may be one person, or a group of people but all of them need to be controlled in their activities.
- 2) **Clear and consistent messages** – All information must be clear in context and not conflicting with other communications. External and Internal communications must not conflict in content, and all must be aligned to the actual disaster response and government directions.

- 3) **Standard Frequency** – The communication team must establish a standard process in which communications are distributed. External and Internal communications need to be released in an organized process and designed for the right audience.
- 4) **No Exceptions** – The communication team must be vigilant in the overall response program and respond to any communications outside of their control. All employees and representatives of the business need to heed to their control and not partake in any rogue communications around the event.

#### **Flexibility in the Initiation of the Plan**

This response plan has been designed to allow the maximum flexibility possible in how the City responds to the emergency at hand. By having both a Business Management Continuity Team and individual Response Teams, the organization can respond to most disasters we are likely to encounter.

#### **Activation of a Designated Hot Site**

Declaring a disaster, which implies recovery at the Hot Site, can be costly for the City due to travel and remote operation requirements. Remote operation can also be traumatic to personnel. Because of the potential variables of an interruption, including the time to repair and/or replace City facilities and infrastructure, management must be prepared to make a “Go” or “No Go” disaster declaration decision in a timely manner.

- **Systems:** The designated Hot Site Facility for basic City operations shall be the Highland County Emergency Management operations center. Upon declaration of a disaster, the Systems Administrator shall contact Highland County EMA coordinator advising the appropriate point of contact of the declared disaster and appropriate arrangements shall be made for data transfer to the recovery site via appropriate data backup media. For client/server computing the servers located at 130 North High Street shall be reconfigured and made available for government use should the site be intact.
- **Business Alternate Location:** Once a disaster has been declared, vital government functions shall be moved to an appropriate offsite location. The offsite location shall be fully

equipped with the appropriate computer and telecommunications infrastructure to sustain limited government functionality.

### **Actual Dissemination of Public Information**

In the event of a government disaster, the designated public information officer shall advise the media that the City government has experienced damage to or outage in its Primary Data Center (or surrounding areas), and that the City officials are evaluating the extent of the damage and the probable cause. Additional information will be provided as soon as details are made available.

If it is known that any City personnel have been injured, this information shall also be included in the preliminary announcement provided that the next of kin have been notified.

### **Disaster Recovery Strategy**

Due to the varying degree of business disruption, the City of Hillsboro has prepared three Disaster Escalation Plans that relate to a minor, intermediate, or major disruption to government business activity.

Escalation Plan One is initiated when the interruption is estimated to be less than one day (24-hours). Due to the limited potential impact to daily business activities, only minor modification to the scheduled work load will be necessary. Escalation Plan Two is declared once the interruption is estimated to be greater than one day (24-hours) but less than three days (72-hours). Modifications will be made to the scheduled work load to permit the highest priority application systems to run. Depending on the extent of the damage, some restoration of system programming and production application data will be performed. Most applications will run at normal levels following the restoration and recovery process.

Escalation plan three will be declared if the perceived interruption to normal business activity is estimated to exceed three days (72-hours) or longer. Once declared, all immediate and essential application systems will be recovered at the designated Hot Site. For purposes of the government risk assessment, a Hot Site shall be defined as "a fully operational offsite data processing facility equipped with both hardware and system software to be used in the event of a disaster or for disaster recovery."

Realizing the potential for data loss and the costs associated with enacting the various escalation plans, it is imperative that the Damage Assessment Team complete and present a damage assessment

report to the Business Recovery Management Team in a timely manner. Once submitted, an appropriate escalation plan will be enacted within two hours after receipt of the damage assessment report.

### **Scope of the Business Continuity Plan**

The purpose of this section is to identify the vital business functions and critical applications that are required for continued operations of the organization following a disaster.

- **Determine Critical Functions**
  - **Police Service**
    - Applications: Maintaining of Civil Order
  - **Fire Service**
    - Applications: Fire and Emergency Medical Service
  - **Street Department**
    - Applications: Road maintenance and general labor
  - **Water/Sewer Maintenance**
    - Applications: Overall maintenance of public utilities
- **Determine Essential Functions**
  - **City Administration**
    - Applications: day to day government business
  - **City Auditor**
    - Applications: maintains organizational finances
- **Determine Necessary Functions**
  - **Water Office**
    - Applications: administers public utility service
  - **Tax**
    - Applications: maintains governmental tax records and payment

### **Establish Recovery Procedures**

This section defines the teams involved in the IT Disaster Recovery effort and their associated responsibilities. The activities are broken down into categories of before, during, and after the disaster.

The established government business continuity plan will consist of several teams, they are: Business Recovery Management Team, Assessment Team, Departmental Interface Team, Equipment and Facilities Team, and the Operations Team. Each of the previously described teams shall be tasked with the following responsibilities.

### **Pre-Disaster Responsibilities**

Each team shall conduct an annual evaluation of the disaster recovery plan for their designated areas. Each team leader shall ensure that their team members thoroughly understand his/her responsibilities in the event of a disaster and that he/she understands the procedures contained within the disaster recovery plan.

### **Disaster Responsibilities**

During a declared disaster, each team shall perform the following tasks:

- Dispatch appropriate team personnel
- Review damage reports and implement Escalation Plan
- Execute final alert/declaration based on severity
- Establish command center
- Provide for well being of team personnel
- Provide overall leadership
- Setup reasonable work/rest schedule for personnel
- Review and oversee any facilities renovation and reconstruction
- Notify administrative level management of status

### **Post Disaster Responsibilities**

Upon resuming normal business operations, each team shall perform a debrief and overall evaluation of team performance. Each team leader shall assess the overall effectiveness of the Disaster Recovery Plan and make appropriate recommendations where necessary. In the event of oversight, each team shall make appropriate revisions to the existing disaster recovery plan and submit the plan to the administrative board for final approval.

### **Conclusion**

No one likes to think about what would happen in the event of a disaster. However, it is truly a reality. Only thorough careful planning and proper documentation can an organization be truly ready in the event a tragedy occurs. This is all part of the process that an organization goes through to create a disaster recovery and business continuity plan. The City of Hillsboro is no exception to this rule. We must be ready in the event of a terrorist attack, internal attack by an employee or even in the event of a natural disaster such as fire, flood or tornado. Through meetings with the users, IT resources and business partners, we've been able to identify the critical systems and the time necessary to recover these systems before business impact is felt. These plans were then translated into a Disaster Recovery Plan (DRP). Once the DRP is implemented and all components completed, the Business Continuity Plan (BCP) will then be implemented and the organizational users can then begin to get government transactions processing again. For the first few days, and even weeks, users will have to operate on a minimum number of systems, with minimum equipment depending on the severity of the disaster. However, as time passes, more and more systems can be brought back on line and more equipment replaced and restored.

In this plan we have examined many topics but there is one theme that is prevalent throughout and that is the key to any successful recovery from a disaster is careful planning. All users need to be involved in brainstorming ideas for the plan but the actual creation of the plan is an IT task. As the DRP is in process, users and business clients need to be thinking about the BCP and what procedures are going to be put in place once the equipment and systems are restored or replaced. This is a key function where IT and Government must work together for the good of the community and ultimately to provide seamless service to the City of Hillsboro.