# A Best Practice for developing your Business Continuity Plan.

The purpose of this document is to provide you guidance in the development of your Business Continuity Plan. Each organization should develop its own plan as we find that “cookie cutter” approaches are rarely effective. A detail risk assessment must be conducted prior to completing the plan, and the plan should be tested at least annually. The following plan sections are for your guidance but may be adjusted to fit your particular needs.

Plan Objectives

The primary objectives of the Plan are:

To provide the organization with a tested vehicle which, when executed, will permit an efficient, timely resumption of the interrupted business operations

To ensure the continuity of the organization's business

To minimize the inconvenience and potential disruption to customers and clients

To minimize the impact to the company’s public image.

1.0 Scope of Plan

The Business Contingency Plan includes the strategies, actions and procedures to resume the business operations and functions associated with the organization. A key portion of this plan is the successful restoration of information systems and communications.

2.0 Plan Assumptions

The Plan should state what assumptions were made in the development of the plan. Plan assumptions are often not documented in the plan process, but are really a vital component. Assumptions are not only appropriate they are necessary. Since there are not many of us who can actually see into the future, assumptions are used to develop the structure the plan is built around.

Assumptions must be made, and documented in the plan, regarding available personnel, available recovery equipment, and estimated damage. The assumptions must have some basis in logic and experience. Management will review and provide input into the assumptions made and advise of changes.

Examples of plan assumptions might include:

In the event of a Level IV failure causing the shutdown of the primary place of business, the Emergency Response Team(ERT) appointed member would be authorized to negotiate temporary workspace sufficient to support employees.

In the event of a Level IV failure, the President of the organization is authorized to activate a $500,000.00 line of credit pre-approved by Big City Bank under agreement 123XYZ on February 12, 2002.

In the event of a Level III failure that renders the main database server inoperable, the IT Manager is authorized to replace this server through the fastest means possible and authorized to expend appropriate funds to this end without requesting additional authority.

3.0 Time Frames

As used in the Plan, "Time-Frame" is the period of time between the occurrence of the disruption event and the time when a given business function must restore some level of service. Time frames define, based on the level of failure, how long it should take to restoration. Time frames should give you a realistic milestone for restoration.

The key here is “realistic.” Don’t create timelines that will look good to management when you are creating the plan. Don’t succumb to pressure to make the number look better. If restoration of a server will take six hours, then putting four on a piece of paper will only create problems elsewhere. If management determines that six hours to recover a server is not acceptable, then the alternative is to deploy technology that can be recovered quicker and accept the cost of doing so.

4.0 Contingency Strategies

Resumption of time-sensitive business operations is dependent on availability of the resources required to support the associated functions and processes. Those resources include:

* Work area for personnel equipped with workstations, printers, networks, and data communications
* Furniture and fixtures
* Voice communications (telephone, inbound lines, long distance, cell phones)
* Connectivity to Mainframe, Midrange, Client/Server and Mini-computer application systems (data communications)

5.0 Disaster Definition

A 'disaster' is defined as the unplanned loss of processing capability, for any reason, for some pre-determined amount of time, as defined by the organization.

6.0 Plan Implementation Phases

The Plan is generally organized into (4) four phases: Response, Resumption, Recovery and Restoration. In the Response Phase, an event has occurred interrupting business processing. The extent of impact to personnel, equipment and facility is to be determined. If a disaster is declared, it is done during the Response Phase. The alternate site is activated, if necessary. The Resumption Phase details the tasks, personnel and equipment necessary to resume mission-critical business functions. The Response Phase details the task, personnel and equipment necessary to resume minimal operations to full business functions. The Restoration Phase provides guidance during the cutover from the alternate processing site and the home site.

7.0 Emergency Response Teams

Recovery personnel are arranged into teams during each phase of the plan. Some teams will participate throughout the plan; some teams will only be activated to perform a specific task for a specific phase. The teams will be composed of a Team Leader, a Backup Team Leader and Staff. Examples of teams include:

Damage Assessment/Salvage Team

Transportation Team

Public Information Team

Communications Team

Specialty Teams

8.0 Team Responsibility

Each team is assigned a detailed list of activities called Tasks. The team is responsible for performing their designated tasks to accomplish a pre-defined objective within each phase. Each phase has specific tasks that need to be accomplished for the orderly recovery of the business function.

9.0 Plan Administration

Administration of the Plan is the responsibility of a designated individual, such as an ERT Coordinator. As the custodian and administrator of the Business Contingency Plan, the ERT Coordinator must have a thorough knowledge of all Plan contents. Responsibility for maintaining specific sections of the Plan resides with each Team Leader in accordance with the Team's objectives and functional responsibilities of Response, Resumption, Recovery and Restoration.

Should a plan review necessitate any changes or updates, the ERT Coordinator is responsible for generating the changes and issuing the updates. Individuals in responsible management positions will be called upon periodically to provide information necessary for maintaining a viable plan and exercise recovery capability.

10.0 Procedures

The primary objective of the ERT Coordinator is to maintain Response, Resumption, Recovery and Restoration information current by promptly processing changes to the Plan. Plan Administration addresses those activities necessary for maintaining a viable Business Contingency Plan.   
Changes to the plan must be promptly processed. Specific Plan Administration activities ensure that the Plan is maintained in a current state, and include:

Conducting regular reviews, at least annually, of the Business Contingency Plan by the ERT.

Developing administrative procedures to control changes within the Business Contingency Plan and to control distribution of the Plan.

Planning, developing, scheduling, and executing exercises to test the Business Contingency Plan, including analysis of test findings.

**Sample Company**

**Business Contingency Plan**

**Last Revised:**

**Sample Company - Business Contingency Plan**

**I. Plan Overview and Definitions**

Plan Design

Overview of the Plan Objectives

Description of Failures Addressed by Plan

Plan Assumptions

Emergency Response Management

Functional Area Recovery Management Teams

Periodic Testing and Plan Evaluation

Emergency Declaration Phase

Alternate Site Activation Phase

Recovery Phase

Application Recovery Categories

**II. Restoration by Functional Area**

Restoration of Information Technology Infrastructure

Staff Responsibilities

Description of operating environment

Network Diagram

Server Configurations

Backup Procedures and Media Retention

Backup Restoration Testing

Management of application media

Workstation Standards

Standard Workstation Configuration

Printer Standards

Power Requirements and Protection

Security

Electronic Mail

Restoration of Accounting

Staff Responsibilities – Assignments

Description of Operating Environment

File Restoration Procedures for MIP

File Restoration for User Work Files

List of required Forms Stored off-site

List of Form Vendors for reorders

List of Employee Contact Information

List of Key Contacts

List of Critical Documents

Restoration of other areas

**I. Plan Overview and Definitions**

**Plan Design**

The Sample Company Business Contingency Plan is intended to provide guidance as to actions management and staff should take in the event of a disaster or other business interruption.

The Plan is a living document and is to be reviewed and updated at least annually. It is the responsibility of the Emergency Response Team (ERT) to activate the plan and to respond to an emergency when it occurs.

**Overview of the Plan Objectives**

Sample Company is critically dependent upon the continuous, uninterrupted services. Any loss of system servers, network communications, or other resources for an extended period of time could have a severe economic impact on Sample Company. This plan will address failures that may occur due to mechanical failure, a force of nature, such as a hurricane or fire, or a brownout or electrical blackout. Other potential sources of failure could be vandalism or sabotage.

The Business Contingency Plan focuses on various levels of disasters, or system failures, and what to do in the event that a disaster occurs. Since it would be nearly impossible to plan for every conceivable type of disaster, the plan defines four levels of failures and the appropriate response to each. Therefore, the plan is less concerned with what caused the failure than the appropriate action to take when the failure occurs. Sample Company will have written, well documented policies and procedures that define acceptable processes, such as backup of data files, server configurations, and workstation configurations that will support this document. The Information Technology Department will also maintain current inventory lists, software license information or contact lists, as supporting documentation to this Plan.

The primary objective of the Business Contingency Plan is to sustain a minimally acceptable level of service for an extended period of time in the event of a business interruption. Should the business interruption be severe, such as the result of storm or fire damage, the restoration period could be extensive before Sample Company is able to return to a pre-disaster level of productivity.

# Description of Failures Addressed by the Plan

Sample Company has defined the following levels of failures, which would adversely impact productivity or cause economic loss to the organization. These are described as follows:

Level 4 Failure – Catastrophic interruption of normal operating processes

Catastrophic failures are the most severe. Level 4 failures typically occur due to natural disasters, acts of war, or criminal actions. Level 4 failures result in the complete loss of critical operating components, such as data and program servers, communications switches and routers, connectivity to outside communication lines, or the loss of the primary place of business.

A Level 4 failure would have a significant economic impact on the ability of Sample Company to continue servicing it customers. Therefore, when a Level 4 failure is declared, the Emergency Response Team (ERT) will activate the Business Contingency Plan.

Should a Level 4 failure occur, and the place of business is not available, Sample Company critical staff will be relocated as described below, until such time as the place of business becomes available, or an alternate place of business is secured. Some Sample Company staff will be utilized to assist in the restoration process and will be required to sign a release for their employee file stating that they are willing and physically able to perform the services requested. This may include carrying and setting up folding tables, offices supplies and equipment.

The Emergency Response Team will determine the severity of the failure and the degree to which the recovery plan is to be implemented. Since some Level 2 and 3 failures may escalate quickly, employees will be advised to listen for news reports and to stay close to their phone or cell phone for further direction. Should staff be asked to exit the place of business for any reason, they will do so immediately and will not return for any reason unless told to do so by their immediate supervisor, or a member of the ERT.

The Emergency Response Team may escalate the priority of a disaster as more information pertaining to the failure is gathered. For instance, a massive failure of the primary data servers would constitute switching to an alternative processing site, or purchasing and installing new servers, very quickly.

A Level 4 failure constitutes a disaster of the highest level and will have the greatest economic impact. It is very important that, in the unlikely event of disaster of this nature, each person knows what he or she is responsible for. Therefore, all staff members are required to read this Plan, as well as the Policy and Procedure manual describing their responsibilities and assignments.

A member of the ERT will be on call at all times. The ERT person on-call, or their delegate, will carry a cell phone or pager for immediate contact. All staff members, fire department, and police will be given this number. Upon determining that a Level 4 failure has occurred, the ERT person on-call is to be contacted immediately. That person has the responsibility of evaluating the extent of the failure, and either activating this plan, or contacting the appropriate resources to resolve the failure.

### Level 3 Failure – Seventy-two hours

A Level 3 failure may be classified as an environmental failure, such as loss of power or air conditioning that would prevent the staff from safely occupying the building for an extended period of time, or a systems failure, such as the loss of network or communication services, preventing staff from accomplishing their tasks.

Sample Company staff will resolve a Level 3 failure in less than seventy-two hours. When a Level 3 failure is identified, the person on-call is to be contacted immediately. This individual will contact the ERT members and determine the appropriate level of response. From that point, the ERT will monitor the failure closely until all services are restored. Level 3 failures could have a significant economic impact on Sample Company, but are not generally as severe as a Level 4 failure, and most of the staff can still function at their workplace. A Level 3 failure generally affects a significant number of mission critical users and, potentially, some users will not be able to access data and program files until full service is restored. Essential staff will fall back to minimal operation levels, and non-essential staff may be called upon to assist with performing tasks manually where possible until full services are restored. A Level 3 disaster normally assumes that the default place of business is available and may be occupied.

# Level 2 Failure – Twenty-four hours

Level 2 failures can be remedied in less than twenty-four hours and are generally not considered to have a high economic impact. However, this may vary by department. For instance, the Loan Origination Department could be adversely impacted if they did not have access to computer programs and files for a 24-hour period during a normal business week.

An example of a Level 2 failure might be a loss of a communications line or network server that brings down all users in a department, or perhaps a truck that runs into the power pole in back of the office, taking down all the voice and Internet data communications to the main office.

In the event of a Level 2 failure that prevents any department from accessing network stored files, that department will fall back to a local workstation, or peer-to-peer network, and resume processing until advised that operations can be returned to normal. A representative of the IT Department will restore the most current files available to local resources and instruct users how to access these files. Before normal services are resumed, IT will move the updated files to the server and assist users in returning to normal operations.

### Level 1 Failure – Four hours or less

Level 1 failures are typically referred to as personal disasters, because they usually only affect one person. A Level 1 failure is resolved in a short period of time, and has a minimal impact on Sample Company.

Examples of Level 1 failures include a printer not functioning, loss of a system component such as a keyboard, mouse, or monitor. An error created by a software application may also result in a Level 1 failure.

Level 1 and 2 failures are the most often recurring failures, and while each individual occurrence will not have the economic impact that a single Level 4 and 3 failure, they can be very costly over a period of time. Therefore, these types of mini-disasters deserve closer attention. Sample Company will institute a manual tracking system for small support requests and repairs and review these monthly for trends that need specific attention. IT will prepare a monthly report to management recounting the number of support calls responded to and actions taken. This Help Desk reporting system will be a part of the Business Contingency Plan process and will be used to identify and deter Level 1 and 2 failures.

# Plan Assumptions

In order for Sample Company and the ERT to respond to the failures, certain assumptions pertaining to critical components and processes must be made. The following lists the assumptions that have been made in preparing this Plan.

#### Primary Place of Business

Sample Company is located at Insert business location here. The primary office number is Insert number here.

INSERT MAP HERE

Operating Structure

INSERT ORGANIZATION CHART(S) HERE

#### Processing or Data Center and Network Infrastructure

INSERT AS DETAIL DESCRIPTION OF TECHNOLOGY INFRASTRUCTURE AS APPROPRIATE HERE.

#### Alternate Site

INSERT AS DETAIL DESCRIPTION OF ALTERNATE PROCESSING SITE(S) TO INCLUDE MAP TO THE LOCATION AND IMAGE OF THE INTERIORS AS WELL AS DIAGRAMS OF WHERE EQUIPMENT IS TO BE PLACED IF POSSIBLE. INCLUDE COMMUNICATIONS AND ELECTRICAL INFORMATION AS WELL AS CLIMATE CONTROL.

Should a Level 4 failure occur that prevents returning to the primary place of business for an extended period of time the ERT will pursue the immediate leasing and setup of business at an alternate site. The ERT would authorize the purchase or lease of either temporary office furniture or permanent replacement furniture and associated office supplies.

# Alternate Site Processing

Should a Level 3 failure occur that would prevent staff from accessing the primary server for a period of up to 72 hours, the ERT would make the determination as to what critical processes needed to be performed and assign those staff as appropriate. IT would purchase or lease workstations and printers to facilitate a system recovery and would load the accounting program and other applications and data from the most current backup tape. The effected area would then operate in a stand-alone mode until normal business operations are restored.

In the event that a Level 4 failure occurs requiring a restoration cycle greater than 72 hours, IT would acquire, or lease, workstations and restore the accounting application, Excel and Word files from backup to individual workstations. Staff would process from a temporary location as described above. IT will restore files from the workstations back to network servers when normal operations are restored.

#### Assignment of Non-Essential Functions

In the event of a Level 3 failure, staff from all departments other than INSERT SPECIFIC DEPARTMENTS HERE would suspend operations for the duration of the crisis.

In the event of a Level 4 failure, some non-essential staff may be assigned to assist in the recovery process. Other staff will not report to work until advised to do so.

#### Acquisition of office furniture, supplies, computer hardware and software

The declaration of the Business Contingency Plan will serve as authorization for the ERT to assign staff to purchase or lease office space, furniture and supplies. Based on the nature of the failure, the ERT person assigned to communications will be authorized to negotiate with a service provider as soon as an alternate long-term site is under contract. ERT staff will retrieve forms from off-site storage and order replacement stock immediately, depending on the anticipated duration of the outage and quantity of stock affected by the disaster.

A representative from IT and INSERT NAME OR POSITION will be responsible for acquiring replacement hardware and software as needed. Sample Company staff will have already been issued company charge cards that may be used, in part, for this purpose. The amount and type of hardware will depend on the nature of the failure. However, recovery will focus first on restoring desktop stand-alone operations. This will mean restoring user images to desktops, loading current data file backups, and testing print operations. IT will acquire printers, small work group hubs, and cables to link work groups together in order to share files and information.

#### Contracted Services

In the event of a Level 4 failure, Sample Company does not have the IT resources to insure a rapid restoration of all services. Therefore, the ERT will have the authority to instruct IT to contract restoration services to third-party vendors. This would include setup of workstations and peer-to-peer networking services, preparing printers, and restoring files. A member of IT would supervise the contracted staff in the restoration process. This would allow IT to facilitate a more rapid restoration of the technology infrastructure.

# Emergency Response Management

Planning for the emergency response in the aftermath of a disaster is a complex task. Preparation for, response to, and recovery from a disaster affecting the functions of the organization requires the cooperative efforts of many support organizations, in partnership with the functional areas supporting the "business" of Sample Company. Management of failures will be handled through the following groups:

Emergency Response Team (ERT)

Area Recovery Management Team(s) (ARM)

The Executive Director, under the direct authority of the Board of Directors, chairs the Emergency Response Team (ERT). The team is composed of senior management, to include:

INSERT NAMES AND POSITIONS HERE

Where appropriate, the Emergency Response Team will assign Area Recovery Management (ARM) Teams to specific areas. ARMs are responsible, along with the ERT, for restoration. Sample Company will create and manage the following ARM teams.

Functional Area Recovery Management Teams

INSERT NAME OF ASSIGNED PERSONS UNDER EACH TEAM, YOU MAY HAVE MORE TEAMS THAN LISTED THERE DEPENDING ON YOUR BUSINESS

Damage Assessment/Salvage

Transportation

Public Information

###### Personnel

Technology

Communications

Safety and Security

Restoration

#### Establishment of the Crisis Management Center

Restoration of mission critical processes is the joint responsibility of the ERT and the ARM teams. ARM teams will work at the direction of the ERT. If the primary place of business is functional, the ERT will establish a central Crisis Management Center (CMC) in the main conference center. The CMC will remain staffed at all times in order to coordinate activities and direct the recovery process.

Should the primary place of business not be accessible, the Safety and Security Coordinator will establish a CMC as close as possible to the primary place of business, either by leasing temporary office space or by renting a trailer or vehicle suitable for the ERT to operate from during the recovery phase, and place the mobile unit near the current office, if possible. Once a temporary place of business is established, the Communications Coordinator will establish voice and data communications to this location.

#### Coordination and Restoration Funding

As soon as a disaster is declared, the ERT chairperson will notify Board Members of the situation and will contact the primary bank to make cash reserves or lines of credit available to fund the recovery process.

#### **Functional Area Recovery Management Teams**

#### The Emergency Response Team (ERT) is responsible for managing and coordinating all aspects of recovery. The members of the ERT are assigned specific tasks for which they are responsible. Area Recovery Management (ARM) teams that facilitate the recovery process support the ERT. This Plan identifies specific ARM teams as follows.

Damage Assessment/Salvage is activated during the initial stage of an emergency. The team evaluates the initial status of the damaged functional area, and estimates both the time to reoccupy the facility and the salvage value of the remaining equipment. This team draws members from functional areas, as well as accounting, information technology, suppliers and vendors. Following the assessment of damage, the team is responsible for salvaging equipment, data and supplies. The team identifies which resources remain and authorizes immediate replacement of items destroyed or unusable. The members of the Damage Assessment Team become the Salvage Team and Replacement Team once the assessment is complete.

Transportation is responsible for arranging transportation for personnel, equipment, and materials to alternative work sites, as necessary. The team members are not expected to move heavy equipment or do work that is hazardous to their health. However, those persons assigned to this team should make the ERT Chairperson aware when assigned if they are not physically capable of lifting light loads, or doing strenuous work. The Chairperson assigns persons unable to assist in lifting or moving office furniture for short periods to other responsibilities. The team will be responsible for contracting with office supply houses, movers, and laborers to assist in the majority of the labor that must be done to set up an office space.

Public Information is the interface with the media, general public, customers and clients of the company. Sample Company will carefully prepare an outline defining what information is to be provided by the Public Information Coordinator. Staff will not make statements to any outside source during the crisis, but will direct inquiries to the Public Information Coordinator.

Personnel are responsible for interfacing with staff during the recovery process. Since some staff members will be reassigned to assist in the recovery process, and others will be relieved of duty until operations are restored, the Personnel Coordinator will be the central point of contact for all questions pertaining to staffing.

Technology is responsible for restoring the technology infrastructure and providing support to staff during the restoration process. A member of the Information Technology Department coordinates the team.

Communications is responsible for establishing voice and data communications between the affected site and the remainder of the organization. This will include rerouting of phone lines, data communications, and so forth.

Safety and Security will, depending on the type of disaster that occurs, be responsible for notifying staff of any safety hazards and for ensuring that the site is secure. The Safety and Security Coordinator will coordinate with fire or police during a disaster, as necessary. The Safety and Security Coordinator is responsible for acquiring temporary facilities in the event the primary place of business is not available.

Restoration team will coordinate the site restoration to include office setup, forms, supplies and the general requirements of a working office.

**Periodic Testing and Plan Evaluation**

On a periodic basis, no less than annually, the ERT must ensure that the plan undergoes a formal review to confirm the incorporation of all changes since the last examination. The ERT will review the Plan on an annual basis, making changes where appropriate. The revised Plan will then be distributed to all authorized personnel, who exchange their old plans for the newly revised plans.

Sample Company will also conduct tests of the Plan on a regular basis, but no less than annually. The documented Standard Operating Procedures (SOP) supports this plan. The Business Contingency Plan depends on documentation and lists of contacts, forms, current vendor information, employee contact lists, as well as hardware and software listings to include licensing information. These lists should be appended to this plan and be readily available. Copies of all lists will also be maintained off-site; in the event a Level 4 failure would make originals unavailable.

# Emergency Declaration Phase

The Emergency Declaration phase begins with the initial response to a disaster; this is the identification of a Point of Failure. During this phase, the existing emergency plans and procedures direct efforts to protect life and property, as the primary goal of an initial response. Security over the area is established with local support services, such as police and fire departments. The chairperson of the ERT is alerted and begins to monitor the situation.

If the emergency situation appears to affect primary processing center(s) (or other critical facility or service), either through damage to the technology infrastructure or support facilities, or if access to the facility is prohibited, the ERT chairperson will closely monitor the event, notifying ERT personnel to begin damage assessment. Once access to the facility is permitted, an assessment of the damage is made by the Damage Assessment/Salvage team to determine the estimated damage and projected length of the outage. If access to the facility is precluded, then the estimate includes the time until the effect of the impact on the facility can be evaluated.

If the estimated outage is less than seventy-two hours, recovery will be initiated under normal operational recovery procedures. If the outage is estimated to be longer than seventy-two hours, then the chairperson activates the ERT, and the Business Contingency Plan is activated. The recovery process then moves into the restoration phase. Under some conditions, it is advisable to notify the ERT that a disaster has occurred even if the failure is expected to be corrected in less than seventy-two hours. The ERT remains active until recovery is complete to ensure that Sample Company will be ready in the event the situation changes.

# Alternate Site Activation Phase

Normally, the Alternate Site Activation phase begins with outages anticipated to be longer than seventy-two hours, or when management deems that the emergency warrants activating alternate site processing. In the initial stage of this phase, the goal is to resume processing of critical applications. Processing may resume either as before or at the designated alternate site, depending on the results of the damage assessment of equipment and the physical structure of the building.

During this period, processing will resume in limited capacity mode. When the ERT elects to move operations to the alternate site, IT will immediately load the most current backup information to the backup server and staff will report to the alternate site. The following people will be responsible for restoring and bringing the operations live:

Information Technology – INSERT RESPONSBILE PERSON

Responsible for reloading files and setting up equipment. IT will locate workstations and work with operations staff to begin processing.

INSERT DESCRIPTION OF EACH ADDITIONAL AREA AND LEAD PERSON

If Sample Company is unable to restore operations at the effected site, the ERT, through the Safety and Security Coordinator, will immediately search for office space suitable for the entire operations. A site will be located and the ERT will coordinate with ARM teams to begin restoration to this site. Team members responsible for communications and transportation will purchase temporary office furniture, equipment, forms and other materials needed. Voice and data communications will be established and operations resumed to the degree possible.

# Recovery Phase

The time required for recovery of the functional areas and the eventual restoration of normal processing depends on the damage caused by the disaster. The time frame for recovery can vary from several days to several months. In either case, the recovery process begins immediately after the disaster occurs and runs continuously until normal operations are restored.

The Recovery Phase incorporates all steps necessary to bring mission-critical functions back up to a service level. This will involve restoring operating systems, applications and data. All information is validated as current before beginning processing. Part of the planning and procedure documentation for this phase includes documenting the time required from the moment that a disaster is declared, and the alternate processing site(s) is activated, until the system is operational. To determine the appropriate order of priority in restoring applications, Sample Company has categorized all software and processes into the following categories, and recovery will begin with Category 1 items and progress through all categories until normal operations are resumed.

# Application Recovery Categories

Category I - Critical Functions are mission critical functions. Sample Company has defined Category 1 functions as:

INSERT LIST OF CRITICAL FUNCTIONAL AREAS

Category 2 - Essential Functionsare those functions that are important, but which may be suspended for a period of time (ranging from three to five days) without having a critical impact on the business. Sample Company has defined Category 2 functions as follows:

Office applications such as word processing or spreadsheet solutions

General Accounting (General Journal, General Ledger, Fixed Assets)

INSERT OTHER FUNCTIONS AS APPROPRIATE

Category 3 - Necessary Functionsare important to the business, but in the case of a catastrophic failure, could be suspended for a period of time or restored after Category 1 and 2 functions are operational. Sample Company has defined Category 3 functions as follows:

INSERT OTHER FUNCTIONS AS APPROPRIATE

Category 4 - Desirable Functionsare those tasks that are a part of day-to-day business, but could be performed manually, by using personal computers not connected to the network, or independently. Desirable functions can be suspended for more than 30 days, without a significant economic impact on the company. Sample Company has defined these as all other functions of the business

INSERT DESIRABLE FUNCTIONS AS APPROPRIATE

# II. Restoration by Functional Areas

# Restoration of Information Technology

#### Staff Responsibilities

INSERT PERSON(S) RESPONSIBLE, AND THEIR FUNCTIONAL RESPONSIBILITY HERE IN APPROPRIATE DETAIL TO EXECUTE RESTORATION.

#### Description of Operating Environment

For Level 1 through Level 3 failures, servers and workstations will be restored or replaced at the primary place of business. IT will replace failed components based on current configurations for Standard Server and Workstation. IT is authorized to purchase replacement components from the fastest and least expensive source, with time to replace being a delimiting factor.

The IT Manager will have a Sample Company credit card and is authorized to facilitate the replacement of failed components. All receipts will be provided to the Controller, along with a description of the conditions that warranted the replacement and other appropriate documents to support the purchase.

#### Network Diagram

The following is a conceptual diagram of the Sample Company network infrastructure. Sample Company will update this diagram as necessary in order for this diagram to represent the most current technology infrastructure.

INSERT NETWORK DIAGRAM AND SERVER DESCRIPTIONS

#### Server Configurations

INSERT DESCRIPTION HERE

# Backup Procedures and Media Retention

INSERT DESCRIPTION HERE

# Backup Restoration Testing

INSERT DESCRIPTION OF BACKUP RESTORATION PROCESS HERE

IT will restore data files from user server directories to selected desktop systems each quarter to verify that files are recoverable and that staff can function from local workstations during a Level 3 or Level 4 failure.

IT will do a random restore of files from backup media to each server in the central processing center(s) on a monthly basis to verify that the media is functional.

#### Management of Application Media

IT is responsible for maintaining a complete list and copies of all licensed software off-site in a secure location. In the event of a catastrophic failure that results in licensing information being destroyed, IT would use this information for the replacement of application media.

IT will also use cloning software to store images of workstation drives for rapid restoration and deployment. Copies of these images will be maintained off-site until needed. IT will test the image restoration no less than annually and will replace images as changes are made to workstations.

# Workstation Standards

The user environment is composed of INSERT DESCRIPTION based workstations from various vendors.

#### Standard Workstation Configuration

The Sample Company workstation configuration is subject to change. The following is a current standard workstation configuration for replacement in an emergency situation.

INSERT CURRENT STANDARD WORKSTATION CONFIGURATION

#### Printer Standards

INSERT CURRENT STANDARD PRINTER CONFIGURATION(S)

#### Power Requirements and Protection

INSERT CURRENT STANDARD UPS CONFIGURATION(S)

#### Security

IT will restore all replacement units to provide for password protection.

#### Electronic Mail

In the event of a Level 3 failure of the Sample Company electronic mail server, the ISP mail services provider will be notified to hold mail until a backup server is restored.

In the event of a Level 4 failure of the Sample Company electronic mail server, IT will “failover” to hosted services provided by the ISP until such time as regular services are restored.

# Restoration of [Insert Department Name(s)]

Staff Responsibilities – Assignments

INSERT RESPONSIBLE PERSONS AND ASSIGNMENTS HERE

Description of Operating Environment

File Restoration Procedures for Core Applications

File Restoration for User Work Files

List of Required Forms Stored Off-Site

List of Form Vendors for Reorders

List of Employee Contact Information

List of Key Contacts (Vendors, Suppliers, Customers)

List of Critical Documents Stored at Primary Place of Business

# REPEAT RESTORATION PROCEDURES FOR EACH DEPARTMENT

## End of Sample Business Contingency Plan