January 1, 20XX

ABC Company

123 Main Street

Los Angeles, CA 90744

(800) ABC-COMP

[www.ABCCompany.com](http://www.ABCCompany.com)

Table of Contents

[I. Purpose of the Business Continuity Disaster Recovery Plan 3](#_Toc360185616)

[II. Business Continuity Philosophy 4](#_Toc360185617)

[III. Policy Statement 5](#_Toc360185618)

[IV. Overview of the Plan 6](#_Toc360185619)

[V. Example Recovery Scenarios 7](#_Toc360185620)

[VI. The Readiness Team 11](#_Toc360185621)

[VII. Major Services, Users, and Key Considerations 16](#_Toc360185622)

[VIII. General Procedures for Potential Interruptions 20](#_Toc360185623)

[IX. Policies For Reducing Risks 27](#_Toc360185624)

[X. Contingency Site Description 30](#_Toc360185625)

[XI. Emergency Action Teams 31](#_Toc360185626)

[XII. Procedures for an Emergency or Disaster 35](#_Toc360185627)

[XIII. Testing and Maintaining the Plan 50](#_Toc360185628)

[XIV. Appendices 53](#_Toc360185629)

[Appendix A – Emergency Notification Lists 54](#_Toc360185630)

[Appendix B – Off-site Storage, Sites, Emergency Control Centers 56](#_Toc360185631)

[Appendix C – Vendor Contacts 57](#_Toc360185632)

[Appendix D – Service Agreements 58](#_Toc360185633)

[Appendix E – Information Systems Equipment Configurations 59](#_Toc360185634)

[Appendix F - Distribution List For This Plan 61](#_Toc360185635)

[Appendix G – Summary of Responsibilities 62](#_Toc360185636)

[Appendix H – Receipt and Acknowledgement 65](#_Toc360185637)

# I. Purpose of the Business Continuity Disaster Recovery Plan

Information systems are an important resource for ABC Company’s (Company) employees. This Business Continuity Disaster Recovery Plan (hereinafter referred to as the “Plan”) documents the strategies, personnel, resources, and procedures required to provide immediate response and subsequent recovery from emergencies and disasters including:

* Unplanned business interruptions
* Loss of critical services (computer processing, telecommunications)
* Loss of building access (contamination, etc.)
* Physical facility catastrophe (fire, sabotage, etc.)

# II. Business Continuity Philosophy

The primary objective of business continuity is to help ensure the operation of ABC Company’s business by providing the ability to successfully continue operations in the event of a disaster or emergency.

Specific goals of the Plan relative to a disaster or emergency include:

* To detail the correct course of action to follow
* To minimize confusion, errors, and expense to the Company
* To effect a quick and complete recovery of services

Secondary objectives of the Plan are:

* To reduce risks of loss of services
* To provide ongoing protection of company assets
* To ensure the continued viability of this Plan

# III. Policy Statement

Company management is responsible for protecting all assets of ABC Company’s organization. These assets include employees, physical property, information, and records relating to the conduct of the business.

Management personnel are specifically responsible for:

* Identifying and protecting all assets within assigned areas of control
* Ensuring that all employees understand their obligation to protect the organization's assets
* Implementing/observing security practices and procedures that are consistent with generally accepted practice and with the specific guidelines stated in this Plan.
* Noting any variance from established security practices and initiating corrective action
* Assigning responsibilities for establishing, maintaining, and coordinating ABC Company’s Information Systems Business Continuity Recovery Plan

# IV. Overview of the Plan

The Plan is a comprehensive document containing the necessary instruction, policies, organization, and information required to be prepared for an emergency or disaster that would affect ABC Company’s information systems. The Plan consists of the following major sections:

* The Readiness Team. This section establishes personnel known as the Readiness Team. This team is responsible for constructing and maintaining this Plan, managing business continuity information systems activities, and for the continued viability of the Plan.
* Major Services, Users, and Key Considerations. This section describes the critical applications, identification of users, and key considerations such as equipment configurations, user work schedules, and processing priorities.
* General Procedures for Potential Interruptions. This section describes the service and general instructions for handling each type of interruption. Typical interruptions include fire, power outage, and telecommunications failure.
* Policies for Reducing Risks. This section includes policies designed to reduce risks of emergencies or disasters occurring, of excessive damage when they do occur, and of failing to recover from an emergency or disaster.
* Contingency Site. This section identifies the Contingency Site and describes the facilities provided.
* Procedures for an Emergency or Disaster. This section describes the instructions and procedures to be followed in the event of an emergency or disaster.
* Maintenance of The Plan. This section contains the policies and procedures needed to ensure that the Plan remains viable as the business environment evolves.

# V. Example Recovery Scenarios

A. Three phases of recovery

The scenario for recovery following an emergency or disaster involves three "phases":

1. The initial response of the Readiness Team
2. Implementing recovery plans
3. Restoring normal operations

Although the three phases occur in every recovery situation, the tasks and the people involved vary according to the nature of the emergency or disaster and its severity.

Following are three example recovery scenarios for understanding the steps involved in recovering from an emergency or disaster. The three examples also illustrate some of the differences in recovery steps and elapsed times for minor, moderate, and major severity:

* Telecommunications failure affects several critical departments
* No commercial power available for five days
* Major fire destroys ABC Company’s offices and network server room

B. Example #1 - partial interruption of services (minor severity)

Scenario: Telecommunications equipment failure affects several critical departments

Elapsed Time

RECOVERY SEQUENCE After Failure

INTERRUPTION OF SERVICE 0 hour

RECOVERY PHASE 1

Initial Response of Recovery Team:

- Problem/repair alternatives evaluated 1 hour

- Interruption of service assessed 1.5 hours

- Decision to implement recovery actions 1.5 hours

RECOVERY PHASE 2

Business Continuity Recovery Plans Implemented:

- Affected users notified 1.5 hours

- PCs in less critical locations are 2 hours

temporarily assigned to the affected users

(requires users to go to other departments)

- Dialup arrangements implemented & tested 3 hours

(for use by a few critical functions)

- Work schedule adjusted for the delay 3 hours

RECOVERY PHASE 3

Normal Telecommunications Service Restored:

- Equipment repaired 24 hours

- Affected users notified 24 hours

- Normal telecommunications restored 25 hours

**TOTAL RECOVERY TIME 25 hours**

C. Example #2 - major failure but network intact (moderate severity)

Scenario: No commercial power available for five (5) days

Elapsed Time

RECOVERY SEQUENCE After Failure

INTERRUPTION OF SERVICE 0 hour

RECOVERY PHASE 1

Initial Response of Recovery Team:

- Problem/repair alternatives evaluated 1 hour

- Interruption of service assessed 1.5 hours

- Decision to implement recovery actions 1.5 hours

RECOVERY PHASE 2

Business Continuity Recovery Plans Implemented:

- Contingency site notified 2 hours

- Activate Emergency Control Center 3 hours

- Emergency Action Teams\* notified and assembled 3 hours

(\* only selected Emergency Action Teams activated)

- Assemble backup tapes, supplies, other needed 3-5 hours

materials and documentation

- Prepare recovery computer(s) for operation 8-24 hours

- Travel to & assemble at Contingency Site 12-48 hours

- Recover any lost work in progress 12-48 hours

- Resume information systems operations on 12-48 hours

recovery basis (probably reduced service levels)

RECOVERY PHASE 3

Network Server Operations Restored:

- Problem resolved at original location 5 days

- Network servers tested 5 days

- Operations transferred back to primary offices 5-6 days

- Operations normalized 7 days

**TOTAL RECOVERY TIME 7 days** D. Example #3 – central network and offices destroyed (major severity)

Scenario: Major fire destroys ABC Company’s offices and network server room

Elapsed Time

RECOVERY SEQUENCE After Failure

INTERRUPTION OF SERVICE 0 hour

RECOVERY PHASE 1

Initial Response of Recovery Team:

- Problem/repair alternatives evaluated 1 hour

- Interruption of service assessed 1.5 hours

- Decision to implement recovery actions 1.5 hours

RECOVERY PHASE 2

Business Continuity Recovery Plans Implemented:

- Contingency site notified 2 hours

- Activate Emergency Control Center 3 hours

- Emergency Action Teams\* notified and assembled 3 hours

(\* all Emergency Action Teams activated)

- Assemble backup tapes, supplies, other needed 3-5 hours

materials and documentation

- Prepare recovery systems for operation 8-24 hours

- Travel to & assemble at Contingency Site 12-48 hours

- Recover any lost work in progress 12-48 hours

- Resume computer service operations on 12-48 hours

recovery basis (probably reduced service levels)

RECOVERY PHASE 3

Replacement Network Server Room Operational:

- New network server facilities established 3 weeks

- New hardware obtained and installed 3 weeks

- New network server tested and made operational 4 weeks

- Operations transferred to new server 4 weeks

- Operations normalized 6 weeks

**TOTAL RECOVERY TIME 6 weeks**

# VI. The Readiness Team

A. Purpose of the readiness team

The purpose of the Readiness Team is to establish and direct plans of action to be followed during an interruption or cessation of information systems caused by an emergency or disaster. As the name implies, the Readiness Team maintains readiness for emergencies and disasters by means of this Information Systems Business Continuity Recovery Plan. The Readiness Team is also responsible for manag­ing recovery activities and can be thought of as the "recovery management team". Through the recovery plans, the Readiness Team provides for:

* The safety of personnel
* The protection of property
* The continuation of business

B. Organizing and planning

The Readiness Team consists of:

* Emergency Coordinator
* Alternate Emergency Coordinator
* Contingency Site Coordinator
* Emergency Action Team Leaders
* Any other designated individuals

The list of designated members of the Readiness Team, showing names and functions, is provided in Appendix A.

The responsibilities of individuals assigned to the Readiness Team are in addition to their regular assignments and are made on the basis of famil­iarity and competence in their respected areas of specialties.

This Plan is administered by the Emergency Coordinator and the Alternate Emergency Coordinator. The Alternate Emergency Coordinator is also responsible for maintaining an Emergency Control Center. Emergency Action Teams are used to facilitate the response to various types of emergency and disaster situations. A Contingency Site Coordinator and Alternate are designated for emergencies and disasters requiring offsite operations at a Contingency Site.

The responsibilities and functions of the Coordinators, Emergency Action Teams, and the Emergency Control Center are discussed in the sub-sections below. Emergency Action Teams include:

* Emergency Action Operations Team
* Emergency Action Applications Team
* Emergency Action Hardware Team
* Emergency Action Facilities Team
* Emergency Action Administrative Assistance Team

See Section XI. Emergency Action Teams which specifically describes each type of Emergency Action Team.

C. Emergency coordinator

The Emergency Coordinator is responsible for developing and coordinating the Readiness Team. During an emergency or disaster situation, the Emergency Coordinat­or will activate and direct all activities until the situation is under control. In the absence of the Coordinator, the Alternate Emergency Coordinator will assume these duties. Additionally, the Emergency Coordinator is responsible for the following:

* Reviewing, evaluating, and updating this Plan at least annually to assure that all emergency and disaster situations have been adequately considered and that appropriate recovery plans and procedures have been prepared.
* Ensuring that the Emergency Readiness Team and other employees receive proper training of recovery plans and procedures. This will routinely be done as a part of annual (or more frequent) tests of the Plan. The Coordinator will also ensure that new employees are properly trained and that certain emergency and disaster procedures are reviewed as frequently as necessary.
* Conducting meetings with the Alternate Emergency Coordinator, the Contingency Site Coordinator, and the Emergency Action Teams as necessary.
* Keeping all members of the Emergency Readiness Team fully briefed on all aspects of the recovery process.
* Evaluating the readiness and proficiency of each Emergency Action Team and the appropriateness of their assignments.
* Keeping management informed of the status of the Emergency Readiness Team and the recovery.
* Communicating the status of emergency and disaster situations to management promptly and efficiently.
* Maintaining liaison with local fire and police agencies, other company locations, and other involved parties as appropriate.

The designated Emergency Coordinator is identified in Appendix A.

D. Alternate emergency coordinator

In the absence of the Emergency Coordinator, the Alternate Emergency Coordinator will assume the duties of the Emergency Coordinator. The following additional duties are assigned to the Alternate Emergency Coordinator:

* Assisting the Emergency Coordinator in maintaining an up-to-date Plan, emergency and disaster procedures, and in directing proper distribution of the Plan.
* Providing emergency evacuation programs and posting them on bulletin boards or otherwise distributing them to all personnel.
* Maintaining up-to-date contact information for Offsite Emergency Coordinator, Emergency Action Team members, emergency telephone numbers, and vendors.
* Activating the Emergency Control Center and administering the Control Center itself during an emergency or disaster situation.
* Keeping the Emergency Control Center properly equipped and in a state of readiness.
* Monitoring all tests of the Plan, and recording the progress, problems, and successes.

The designated Alternate Emergency Coordinator is identified in Appendix A.

E. Contingency site coordinator

The Contingency Site Coordinator is responsible in helping to establish and maintain written procedures to be followed during emergency or disaster situations requiring opera­tion at a Contingency Site. During such an emergency or disaster, the Contingency Site Coordinator will direct opera­tions at the Contingency Site and communica­te with the primary location via the Emergency Control Center. In the absence of the Contingency Site Coordinator, the Alternate Emergency Coordinator will assume the duties of the Contingency Site Coordinator.

In addition, the Contingency Site Coordinator is responsible for the following:

* Periodically reviewing and evaluating the Plan to assure the Contingency Site has been adequately prepared.
* Assuring that the Contingency Site meets the minimum requirements for testing and recovery purposes.
* Overseeing periodic tests at the Contingency Site and maintaining technical readiness for operation of services from the site.
* Recommending to the Emergency Coordinator any necessary changes or improvements in the Plan.
* Keeping the Emergency Coordinator informed of the status of the Contingency Site and any changes relative to requirements or planning.
* During emergency or disaster offsite operations, communicating the status of operations via the Emergency Control Center.
* Assuming responsibilities of the Emergency Coordinator in the event that both the designated Emergency Coordinator and the Alternate Coordinator are unavailable for duty.

The designated Contingency Site Coordinator is identified in Appendix A.

F. Use of emergency action teams

Emergency Action Teams are used for specific functions during an emergency or disaster situation and subsequent recovery. The teams and their responsibilities are defined in Section XI Emergency Action Teams. Members of Emergency Action Teams are identified in Appendix A.

In general, the Team Leader of each Emergency Action Team is responsible for the following duties:

* Periodically reviewing and evaluating the emergency and disaster planning with particular emphasis on completeness and accuracy of specific recovery procedures.
* Each Emergency Action Team’s responsibilities, assignments of and changes in personnel, and availability of equipment, facilities, and services.
* Recommending to the Emergency Coordinator any necessary changes or improvements in the Plan.
* Recruiting and training personnel for emergencies and maintaining proficiency at a high level. All Emergency Action Team members must be capable of performing their duties quickly under stress.
* Informing the Emergency Coordinator of any additions or changes of individuals assigned to an Emergency Action Team.

G. Emergency control center

In an emergency or disaster, the Emergency Control Center will be established from which all communications and activities will be directed. The Emergency Control Center will be used to coordinate the management of recovery procedures, and will serve as the center of all communications between the Emergency Coordinators, the Emergency Action Teams, and all other personnel. The administration of the Emergency Control Center is the responsibility of the Alternate Emergency Coordinator.

The designated Emergency Control Center and alternate locations are identified in Appendix B. The Emergency Control Center is activated when an emergency or disaster has occurred, particularly when the personal safety of employees or property is jeopardized. Readiness and activating of the Emergency Control Center are the responsibility of the Alternate Coordinator. Directing activities and communications from the Emergency Control Center is the responsibility of the Emergency Coordinator.

The Emergency Control Center provides centralized and coordinated control of communications during emergencies and disasters. When the Emergency Control Center is in operation, Emergency Coordinators and Action Team Leaders will coordinate with the Emergency Control Center and keep it informed of status and progress.

If conditions warrant closing of facilities, the Emergency Control Center will communicate the closing notice through the management chain to all employees.

# VII. Major Services, Users, and Key Considerations

A. Purpose of major services, users, and key considerations

It is necessary to the well-being of Company that critical applications pro­cessed on internal (in-house) and external (outsourced) information systems be kept in service even in the event of an emergency or disaster. Critical applications include:

* Accounting (internal)
* E-mail (internal)
* Internet access (external)
* BAS
* Phones
* Active Directory

Each critical application processed internally and externally is described here in terms of the key considera­tions in a recovery scenario.

B. Internal services and applications

The following services are processed on internal information systems:

|  |  |  |  |
| --- | --- | --- | --- |
| **Department** | **Representative(s)** | **Process** | **Time when issue becomes High priority** |
| Accounting/Finance | XXXXXX | Accounts Payable  Lack of info for decisions | 1 week  2 weeks |
| Production | XXXXXX | Process  Paid once per week | 3 days |
| Customer Service | XXXXXX | Inbound call center phones | 4 hours |
| Human Resources | XXXXXX | Payroll on processing day  Benefits | 2 hours  3 days |
| Sales | XXXXXX | Receipt of RFP via email  Claims inquiries | 1 day  1 week |

Software applications processed on internal systems include:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Application Software** | **Server Name** | **Databases used** | **Full backup** | **Stored Off-site** | **Recovery time** | **IT Priority** |
| Active Directory | XXXXXX |  | Yes | Yes | 4 hr | High |
| Internal Domain Name Server | XXXXXX |  | Yes | Yes | 4 hr | High |
| External Domain Name Server | XXXXXX |  | Yes | No | 4 hr | High |
| Exchange Mail Server | XXXXXX | Exchange | Yes | Yes | 4 hr | High |
| Production application | XXXXXX | XXXXXX | Yes | Yes | 8 – 12 hr | High |
| Web Server | XXXXXX | XXXXXX | Yes | No | 6 hr | High |
| Backup Server | XXXXXX |  | Yes | Yes | 6 hr | Medium |
| File Server | XXXXXX |  | Yes | Yes | 12 – 24 hr | Medium |
| Print Server | XXXXXX |  | Yes | Yes | 4 hr | Medium |
| Fax Server | XXXXXX |  | Yes | Yes | 8 hr | Medium |
| VPN Server | XXXXXX |  | No | No | 4 hr | Low |
| Accounting | XXXXXX | Yes (many) | Yes | Yes | 8 hr | Low |
| Voicemail Server | XXXXXX |  | Yes | No | 12 – 24 hr | Low |

C. External services and applications

Third party service providers include:

|  |  |  |
| --- | --- | --- |
| **Vendor** | **Service provided** | **IT Priority** |
| Vendor | Internet and Phone Service Provider | High |
| Vendor | Tape backup off-site storage | High |
| Vendor | Accounting system support | Medium |
| Vendor | Voicemail System Support | Low |

|  |  |  |  |
| --- | --- | --- | --- |
| **Service provider** | **Importance  (high, med, low)** | **Recovery time objective** | **Recovery point objective** |
| Provider 1 | High | 1 day | N/A |
| Provider 2 | High | 3 days | 3 days |
| Provider 3 | Low | 1 week | N/A |
| Provider 4 | High | 3 days | N/A |
| Provider 5 | High | 1 week | 1 week |

D. Information systems equipment considerations

Application software runs on an internal network server computer with numerous PCs and printers directly connected to ABC Company’s network. In recovery situations, the minimum equipment configuration is identified in Appendix E.

E. Special considerations

The following special equipment considerations are necessary components to a successful recovery effort. Each employee is assumed to require:

* Desk
* Computer
* Phone
* Printer
* Internet access
* Email access

User department work area requirements include:

|  |  |  |
| --- | --- | --- |
| **Department** | **Minimal staff required** | **Other resources required** |
| Accounting/Finance | XX | Checks stored off-site |
| Production | XX |  |
| Customer Service | XX | Fax, copier |
| Human Resources | XX | Facilities for staff |
| Sales | XX |  |

# VIII. General Procedures for Potential Interruptions

A. Purpose of general procedures for potential interruptions

This section includes a series of recovery plans that identifies prompt and appropriate actions to take in potential emergencies, disasters, or events causing inter­ruption of information systems. Training sessions are to be held periodically to familiarize employees with these procedures and to outline responsibilities in the event of such emergencies. *The Emergency Coordinator will arrange these training ses­sions.*

*Copies of this Plan must be kept in key locations for ready reference. Members of the Readiness Team must be given copies of this Plan. The Distribution List is contained in Appendix F.*

Assets of the Company are extremely important to its very existence. The most important asset is ABC Company’s personnel. Risks must not be taken to save other assets where personnel may be in jeopardy.

B. Recovery plan for fires

Preventing Fires

* Periodically, review all areas of responsibility for combustible materials.
* Check operational areas before employees leave each day.
* Educate the staff, and new employees, about the fire plan. All employees must have periodic reviews of the fire plan on a schedule to be determined by Company management.
* Regular site inspections which include general area review, and checks of electrical connections, fire extinguishers, and smoke detectors must be made every 12 months by The Alternate Emergency Coordinator.
* Smoking is only allowed in areas designated by Company management. Other areas involving quantities of combustible materials must be reviewed and posted for NO SMOKING, if necessary.

Detecting Fires

ABC Company’s offices have a fire detection and suppression system. Smoke detectors are located in/on the ceiling. If smoke is detected, horns will sound and emergency evacuation should begin.

Extinguishing Fires

* Company management will arrange employee fire extinguisher training. The Alternate Emergency Coordinator must arrange to have all extinguishers inspected annually.
* An employee should only attempt to extinguish a fire if it is very small or confined to a particular piece of equipment. Otherwise, the fire department should be called by the receptionist and the building should be evacuated immediately.
* DO NOT PLAY HERO. If the fire is of any consequence, leave the build­ing immediately.

Evacuating If Fire

* If the fire is such that employees must evacuate the building, a member of the Emergency Action Operations Team should notify the receptionist to call 911 to contact the fire department.
* Employees should not take backup media with them when they evacuate the building. A member of the Emergency Action Operations Team stores backup media offsite on a rotating basis.
* Before evacuation, a member of the Emergency Action Operations Team must shut off all power to equipment and over­head lights. If there is time, Emergency Action Operations Team employees should power down system(s) before cutting power.

Goals

* Protect the lives and health of employees
* Protect essential documents, records, and data
* Minimize damage to data processing equipment and other property

Procedures for Fires

* A member of the Emergency Action Operations Team should notify the receptionist to call 911 and contact the fire department immediately. Give the following information:

Your Name

Your Department and location

Nature of Emergency

* The receptionist will provide 911 with the building address, the location of the fire, and type of fire it is (paper, electrical, etc.).
* If time permits, a member of the Emergency Action Operations Team will shut down systems
* A member of the Emergency Action Operations Team will cut off all electrical power
* If the fire is small, use a fire extinguisher after you have notified the receptionist to call 911. Pull the pin on the fire extinguisher, then discharge the extinguisher by aiming at the base of the fire using a side-to-side sweeping motion.

C. Recovery Plan For Electrical Outages

An electrical outage is most likely caused by a failure of the public electricity utility. In most cases, return of electricity is usually within a few hours, but the Emergency Coordinator is responsible to contact the electricity company to determine how long the outage is expected to last.

Ordinarily, it is necessary to wait until electricity is restored with the possibility that repairs to data files will be necessary. In the unlikely event that electricity cannot be restored for days, then the Emergency Coordinator will contact Company management and coordinate electricity with the Emergency Action Facilities Team.

Procedures For Electrical Outages - If an electrical problem exists, even though public power is not out of service, such as after restoring electricity, the following need to be noti­fied by the Emergency Action Facilities Team:

* Emergency Coordinator
* Electricity Company

D. Recovery plan for telecommunications failures

Failures of the computer telecommunications system fall into two basic categories:

* Hardware Failure - When a piece of telecommunications equipment fails, it must either be repaired or replaced, like any other hardware failure. Faulty or damaged equipment will be replaced as needed.
* Line Failure - The line is a utility service provided by a communica­tions carrier company. If a line fails, just as in an electrical outage, ABC Company is dependent on the utility to fix the problem and restore service. However, if the entire phone system is down in the area, recovery plans must be considered if the outage is predicted to be of long duration. If the outage is predicted to last so long as to affect business operations seriously, the Emergency Coordinator must consider switching operation to ABC Company’s Contingency Site.

An extreme phone system outage will affect the entire business opera­tion, in which case the Contingency Site is one option for temporarily operating the business or some key portions of the busi­ness until repairs are made. See Section X Contingency Site for specific site information.

Procedures For Telecommunications Failures

* Obtain replacement equipment if Company experiences a telecommunications hardware failure
* Notify telecommunications provider a line failure occurred and the circuit is down
* Use dial-up lines at main office or high speed line at Contingency Site

E. Recovery plan for flooding

Preventing Floods - The facility design must be reviewed at least annually by the Alternate Emergency Coordinator for knowledge of risks relative to flooding. The Alternate Emergency Coordinator must know where water pipes and drains are in respect to information systems equipment. If possible, route pipes and add drains to reduce the risk of flood­ing. Know what the potential is for flooding from above (upper floors or roof).

The Alternate Emergency Coordinator must know how the server room facility lies physically in respect to external floods coming in and what steps to take to prevent flooding. If the opportunity arises to choose a new server room, Company management should take into account the flood plain and building construction.

During heavy weather conditions, particularly rain, the Alternate Emergency Coordinator will inspect windows and roofs in proximity to the server room for flooding or water buildup. The Alternate Emergency Coordinator, or contract maintenance staff, must inspect at least twice annually all pipes and valves in proximity to the server room for leaks.

Detecting Floods - The detection of water within the server room is vitally important to prevent electrical shocks, short-circuits, or equipment damage.

Evacuating If Floods

* If flooding is such that employees must evacuate the building, the Emergency Action Operations Team should notify the receptionist to contact the Emergency Action Facilities Team.
* It is not necessary to take backup media with you when evacuating the building. All systems are backed up offsite on a frequent enough basis to make recovery possible from tapes stored at the offsite storage location.
* Before evacuating, all power must be shut off to equipment and over­head lights. If there is time, the Emergency Action Operations Team should power down system(s) before cutting power.

Goals

* Protect the lives and health of employees
* Protect essential documents, records, and data
* Minimize damage to data processing equipment and other property

Procedures for Flooding

* A member of the Emergency Action Operations Team should notify the receptionist to call the Emergency Action Facilities Team immediately. Give the following information:

Your Name

Your Department and location

Nature of Emergency

* The receptionist will provide the building address and the location and type (pipe, roof, etc.) of flooding.
* If flooding is such that there is no risk of electrical shock (i.e. the flooding has just started), a member of the Emergency Action Operations Team must power down the system(s) before cutting power.
* If time allows, the Emergency Action Operations Team must do all that is possible to protect the equipment. If flooding is coming from overhead, the Emergency Action Operations Team must drape the equipment with heavy plastic.
* If flooding is such that employees should evacuate the building, the receptionist must notify Company management immediately.

F. Recovery plan for hardware failures

Appendix E provides a list of information systems equipment used by Company. In most circumstances, the hardware can be repaired to restore operation within a short period of time. Even if the downtime were as long as a day, the preferred approach is to allow the engineers to make their repairs in the normal manner.

Hardware failures generally require either repair or replacement. Specific recovery plans are outlined below.

Network Servers - In the event that a network server is out of service for an extended period of time, such that Company will be seriously affect­ed, the Emergency Coordinator will coordinate with appropriate vendors to correct or replace.

Peripherals And Other Equipment - Peripherals are devices that are attached externally to network servers (e.g. printers, scanners, external tape drives, etc.). Other devices, such as Fax machines and copiers may not be connected to the network but are needed for other functions. Should a hardware failure be prolonged for an extended period of time, the operation of the dependent user department will be seriously affected.

Procedures For Hardware Failures - Appendix C provides a complete list of network server and peripheral vendors. These vendors can assist in determining loaner equipment availability as well as timeframe to obtain replacement parts and/or new equipment.

G. Recovery plan for software failures

Desktop, operating system, and other systems software may encounter errors that result in system downtime. Equipment vendors and software manufacturers can assist in restoring systems to normal functionality. Software manufacturers frequently provide bug fixes and software patches for known problems. Appendix C provides a list of software vendors.

The Contingency Site Coordinator approves the installing of changes provided by software manufacturers. Should changes cause a serious failure of network services, the Contingency Site Coordinator will take the appropriate action to correct the problem either by authorizing a manufacturer-provided "fix" or by designating that the system software be returned to the version prior to loading the changes.

It is very unlikely that system software could cause a major service failure. However, in such an event, the Contingency Site Coordinator will oversee restoring the software from the appropriate backup.

Applications Failures - Some of ABC Company’s applications packages were acquired from third-party sources and are maintained by those companies. These vendors can assist in correcting application problems. Appendix C provides a list of application software vendors.

Applications software is very similar to systems software concerning fail­ures of new versions of the programs. In-house change control proce­dures must be developed to provide for adequate testing before making changes and for backing out the changes if problems are detected.

However, a more serious type of application failure is one where, through error of a program, a user, a maintenance programmer or by other means, data is caused to be incorrect to the degree that business consequences are serious.

In this case, the staff that supports the failed application must determine how the erroneous data will be corrected. Backups of data files may or may not be useful depending on the amount of time elapsed during which the error proliferated. In serious cases, special­-purpose programming may be required to repair the data. In the worst case, the original source transactions will be re-input to recreate the data files.

# IX. Policies For Reducing Risks

A. Protecting data

Information systems data is protected by combing backup and offsite storage procedures. Backups copy the data from disk to removable media (usually magnetic tape) so that data that is lost or damaged for any reason can be restored. Offsite storage for magnetic tapes (or other forms of information) protects the data if the information system itself is destroyed. No business is likely to survive if its vital records are destroyed. Recovery is possible when an information system is destroyed but the data is protected at another location.

B. Backup procedures

The backup procedures for information systems data are as follows:

* Full backups of critical data are completed on a daily basis
* Once a week (Fridays), backups rotated offsite
* Special backups for legal records purposes should be performed as required, usually once each year (January).

C. Backup storage procedures

Backup tapes are stored both on-site and offsite. On-site storage con­sists of tapes located in the media safe in the IT office. The offsite storage facility for network recovery is fully identified (name, location, etc.) in Appendix B.

The backup storage procedures are as follows:

* Nightly backups stored on-site through a weekly rotation
* Weekly full backups stored offsite after they are on-site for a week
* Full backups kept with a rotation
* Special backups, including legal records archives, should be kept offsite for a period of seven to ten years, depending on the contents and purpose of the backup

D. Protecting network servers

Procedures for protecting ABC Company’s network servers:

* Physical security. The computer room remains locked at all times and only the Emergency Coordinator, Alternate Emergency Coordinator and Company management have keys.
* Electronic component damage. Damage due to electrical spikes, surges, over-voltages, and under-voltages reduced by an uninterruptible power supply (UPS) system with power surge protection.
* Security. Strictly adhering to ABC Company’s “Policies and Guidelines On The Use of Information Systems” and “Policies and Guidelines To Secure Information Systems” document procedures protect ABC Company’s information systems.

E. Protecting vital records

Many documents and records are vital to the operation of Company. Company has implemented procedures and plans to protect these vital records. Vital records (checks, invoices, journal entries, etc.) may be required in order to recreate lost electronic data.

Company management specifies how long records must be retained for practical and legal requirements. The schedule is reviewed by the Emergency Coordinator to ensure aspects of the Plan adhere to ABC Company’s retention schedule.

Many vital records are backed up by the network server data backup procedures. Other records, if destroyed, could be re­placed by contacting vendors or other sources. Appendix C provides a list of vendor contacts.

F. Backup of data, hardware, supplies & documentation

All data, spare hardware, supplies, and documents identified as critical for ABC Company’s recovery process, are stored in offsite storage. The offsite storage location is identified in Appendix B. Backups stored offsite include:

* Computer data and software. All data resident on the network server(s), including systems software and applications software, are backed up on a routine basis. The Contingency Site Coordinator is responsible for observing backup procedures at the Contingency Site.
* Critical spare hardware items. A Contingency Site can be used in the event the primary network server is no longer operational. See Section X Contingency Sites. Planning for special peripheral and telecommunications equipment is described in Appendix E. The Alternate Emergency Coordinator is responsible for reviewing backup procedures. Additional equipment such as PCs, printers, Fax machines, copiers, etc. are readily available and are not backed-up at an offsite location.
* Critical operating supplies. Critical supplies, including special forms and items for the Emergency Control Center, are stored in offsite storage. If Contingency Site operations are required, enough supplies will be available to continue operations until more supplies can be obtained from ABC Company’s vendors. The Alternate Emergency Coordinator is responsible for backing up operating supplies offsite.
* All critical documentation. Critical documentation is backed up offsite to assist recovery. Documents that should be main­tained in offsite storage include this Plan, system startup and shut down procedures, and a copy of the relevant passwords.

G. Insurance

All property of the Company, including information systems equipment, is insured under ABC Company’s insurance program. This policy insures the replacement value of the property against most natural kinds of damage or destruction, but does not cover the cost of lost business or replacing lost records.

The information systems equipment is not separately scheduled, but the total coverage must be sufficient to cover the equipment even if it were totally destroyed along with the other property of the organi­zation. The Emergency Coordinator is responsible for informing Company management of the acquisition of new equipment and its value, and to verify annually the accuracy of the information.

# X. Contingency Site Description

A. Emergencies and disasters

An emergency or disaster may require activation of the Contingency Site if information systems are unable to operate. Reasons may vary from actual destruction of the server room to less severe circumstances that affect information systems while leaving the server room intact.

If necessary, equipment will be replaced by the appropriate vendors on a time and materials basis. No prior approval is needed to purchase the replacement equipment. Follow the normal Company policy regarding accepting vendor equipment approving invoices. In the event equipment needs to be replaced, start the process by placing a telephone call to the appropriate vendor(s). Appendix C contains a list of vendor contacts.

B. Contingency site space and resource requirements

The Contingency Site contains office and server room space and related resources as identified below:

* Total person capacity
* Emergency Action Operations Team support staff
* PCs
* Printers
* Fax machines
* Telephone lines
* Internet connectivity
* Security features: lockable cabinets for sensitive documents/forms
* Facilities: locks on doors
* 24 hour access to Contingency Site

C. Recovery plan testing

The Emergency Coordinator schedules tests of the Contingency Site. Tests must observe the following schedule restrictions:

* Tests must be coordinated with the Contingency site – recommended annually
* Actual emergency situations take precedence over tests
* User departments are limited to 6 hours of test time each day
* Emergency Action Operations Team is allocated 6 hours of processing, backup, and administrative time each day

# XI. Emergency Action Teams

A. Responsibilities of the emergency action teams

The following Emergency Action Teams have been defined for use in disas­ters or major emergencies. The purpose, responsibilities, and members of these Teams are described on the following pages. The Teams will be activated selectively by the Emergency Coordinator and/or the Readiness Team accord­ing to the nature of the emergency. The Teams report to the Emergency Coordinator, or the Contingency Site Coordinator if offsite.

Emergency Action Teams:

* Emergency Action Operations Team
* Emergency Action Applications Team
* Emergency Action Hardware Team
* Emergency Action Facilities Team
* Administrative Assistance Team

The use of Emergency Action Teams and the general responsibilities of Team Leaders are discussed in Section IV The Readiness Team. Designated Team Leaders and members of each Emergency Action Team are identified in Appendix A.

B. Emergency action operations team

The purpose of the Emergency Action Operations Team is to ensure resuming of information systems and related processing following an emergency or disaster. The Emergency Action Operations Team oversees processing at the Contingency Site until such time that operations can resume at the original or replacement network server room.

Responsibilities Of The Emergency Action Operations Team

* Periodically review and evaluate the appropriateness and completeness of procedures for backups, offsite storage, and recovery. Backups must include data, software, forms and other supplies, and operations documentation.
* In an emergency or disaster, obtain all appropriate backups from offsite storage, including tapes, supplies, and documentation.
* Participate in initiating operations at the Contingency Site. Then continue recovery operations until the Contingency Site is no longer required. This will require communication with the other Teams to understand levels of service and functional differences in the recovery mode, with the user departments to prepare a revised processing schedule, and with the Offsite or Emergency Coordinators concerning status of work.
* Coordinate with users on how to submit input to and receive output from the Contingency Site.
* If recovery operations continue for an extended period of time, ensure that adequate levels of operating supplies are maintained at the Contingency Site.
* Provide manpower to support the offsite operations. Coordinate with the Emergency Action Administrative Assistance Team for transportation and housing of the Emergency Action Operations Team staff. Revise schedules as appropriate to the needs of the emergency situation.

C. Emergency action applications team

The purpose of the Emergency Action Applications Team is to ensure proper functioning of the applications at the Contingency Site. The Emergency Action Applications Team also coordinates with users on how applications should be operated during the recovery period.

Responsibilities Of The Emergency Action Applications Team

* The Emergency Action Applications Team must participate in preparing and conducting tests at the Contingency Site. If a problem exists on how an application will operate at the Contingency Site, the Emergency Action Applications Team must prepare and document solutions for the problem. Applications documentation and a copy of Plan should be stored offsite.
* In an emergency or disaster, obtain offsite documentation and a copy of Plan from the Emergency Action Operations Team in order to assist in restoring Contingency Site operations.
* Coordinate with the Emergency Action Operations Team and users to determine work that was in progress at the time of the disaster. When operations are restored at the Contingency Site, the Emergency Action Applications Team must first help recover any lost work that was in progress.
* Once user work has been recovered, coordinate with the users about any changes in the way they will interface to their applications and provide assistance as necessary.

D. Emergency action hardware team

The Emergency Action Hardware Team is responsible for repair or replacement of computer hardware, installing and testing computer hardware, and all hardware planning - whether at the original site, the replacement site, or the Contingency Site. Unless a separate Emergency Action Team is established, the Emergency Action Hardware Team is also responsible for telecommunications.

Responsibilities Of The Emergency Action Hardware Team

* Participate in evaluating and selecting ABC Company’s Contingency Site(s), testing at the Contingency Site, and all hardware-related planning.
* In an emergency or disaster, assess the extent of damage or the effect of failures on hardware and telecommunications.
* Coordinate with vendors in obtaining necessary repairs or replace­ment of hardware. Agreements should be negotiated in advance wherever possible for rush delivery of equipment or telecommunica­tions facilities.
* Coordinate with purchasing, finance, insurance, and other depart­ments in equipment salvage, insurance claims, and financing for replacement equipment.
* Install and test all new/replacement hardware or data lines, and supervise all problem solving.

E. Emergency action facilities team

The purpose of the Emergency Action Facilities Team is to restore or replace the server room and other information systems facilities following an emergency or disaster.

Responsibilities Of The Emergency Action Facilities Team

* Maintain current configurations of the information systems facilities. The configurations should include space layouts, lists of all facilities, such as air condi­tioning, power distribution, power conditioning, etc., and specify model numbers, capacities, electrical requirements, etc.
* In an emergency or disaster, assess the damage and recoverability of the facilities. If the facility is usable, proceed to organize immediate repairs.
* If the facilities are destroyed and not usable, locate replacement facilities that can be acquired quickly and are usable for a reasonably long period, if not perma­nent­ly. Facilities include not only requisite square footage in a building, but also cabling, air conditioning, power, etc.
* Coordinate with facilities vendors the build out, equipment, installation, and permits. If possible, negotiate facilities space in advance.
* Coordinate with purchasing, finance, insurance, legal and other departments in ordering new equipment, contracting for space and build out, insurance claims, and financing new facilities.

F. Emergency action administrative assistance team

The Emergency Action Administrative Assistance Team is responsible for all activities in the recovery process that are not handled by other Emergency Action Teams. These activities include arranging transporta­tion, housing, shipping, etc., and performing clerical and other administra­tive functions.

Responsibilities Of The Emergency Action Administrative Assistance Team

* Develop and review administrative procedures of the Plan
* Participate in tests of the Plan to actually perform the administra­tive functions and evaluate procedures and requirements
* Handle all administrative arrangements for transporting, housing, shipping, expense advances, etc.
* Assist in facilitating arrangements and administrative approvals with other departments.
* Perform clerical and administrative functions as needed during the recovery

# XII. Procedures for an Emergency or Disaster

A. Notifying the readiness team

The following recovery steps are for use in an emergency or disaster of a serious enough magnitude to require computer processing to be moved to a Contingency Site. A critical aspect of recovery is the quick reaction of the Emergency Readi­ness Team. The Readiness Team must notify appropriate personnel so that recovery can initiate as quickly as possible.

The Emergency Coordinator has established and will maintain the Emergency Notification List and will ensure that all key person­nel have it available. The Emergency Notification List is contained in Appendix A.

In the event of an emergency or disaster, the following notifying procedures must be followed:

* The Emergency Coordinator should initiate the notification process as soon as possible. If no operations personnel are on duty, a security guard has been provided with the proper procedures and must notify the Emergency Coordinator who will then initiate the notification process.
* The Emergency Coordinator is at the top of the Emergency Notification List. If the Emergency Coordinator cannot be reached, the Alternate Emergency Coordinator must be contacted.
* The first member of the Readiness Team notified is responsible to notify other members of the Readiness Team and to initiate action. The initial action will be to assemble the Readiness Team at the Emergency Control Center or the Alternate Emergency Control Center.

B. Initial readiness team procedures

Once the Readiness Team has been notified, they must proceed to make an immediate assessment of the situation and to initiate appropriate actions.

Readiness Team Procedures

* The first member of the Readiness Team notified is responsible for notifying other members of the Readiness Team and to initiate action. The initial action should be to assemble the team at the Emergency Control Center or the Alternate Emergency Control Center.
* If the Emergency Coordinator has not yet been reached, the Alternate or persons listed next on the Emergency Notification List will assume full responsibilities of the Emergency Coordinator, until he or she has arrived and been fully briefed. The Emergency Coordinator or Alternate Emergency Coordinator will implement the recovery plans.
* The Emergency Coordinator will make an assessment of the situation directly at the scene if possible, or if not, indirectly based on reported information from the notifica­tion sources.
* Based on the Readiness Team's assessment of the situation, the Emergency Coordinator will determine the severity of the problem and decide on the appropriate action.
* If the Readiness Team judges the emergency to be a major disaster, members of the Readiness Team, as directed by the Emergency Coordinator, must do the following:

Activate the Emergency Control Center

Notify the appropriate Emergency Action Teams

Notify Company management

Notify the offsite storage site

Notify the Contingency Site

* The appro­priate correction or recovery plans will be implemented according to the severity of the emergency or disaster.

C. Activating the emergency control center

In the event of an emergency or disaster, a centralized control center will be established from which all communications and activities will be directed by the Emergency Coordinator. In the event that an alternate location becomes necessary, the Alternate Emergency Control Center will be used. The locations of the Emergency Control Center and Alternate Emergency Control Center are identified in Appendix B.

Emergency Control Center Procedures

* The Alternate Emergency Coordinator maintains an Emergency Control Center in a state of readiness. The Emergency Control Center is equipped with table(s), chairs and a telephone. If necessary, certain emergency supplies are backed up offsite along with other emergency materials.
* When the Emergency Coordinator has declared a major emergency, the Alternate Emergency Coordinator will proceed to take all steps necessary to activate the Emergency Control Center.
* The Emergency Coordinator selects either the primary or Alternate Emergency Control Center. For either site, Company management has requisite keys and other items, including names, addresses, and phone numbers, necessary to gain access to the site(s).
* If necessary, telephones will be ordered from the telephone company for emergency installation, and supplies obtained from backup or other sources to properly equip the Emergency Control Center.
* The Emergency Coordinator will notify the Readiness Team of the location and telephone numbers of the Emergency Control Center.

D. Notifying action teams and company management

In the event of an emergency or disaster, the Emergency Coordinator must notify the Emergency Action Teams and Company manage­ment of the incident. Company management needs to know about the emergency and the current status of personnel, property, etc. The Action Teams are intended to carry out very specialized functions in a recovery situation, and will be called in to act according to the incident.

Procedures For Notifying Action Teams And Company Management

* The Emergency Coordinator must determine which Emergency Action Teams should be activated.
* The Emergency Coordinator must notify Company management and if the presence of Company management is required to support the emergency activities or recovery procedures.
* The Emergency Coordinator or his or her Readiness Team designate must notify the Emergency Action Teams.
* Company management, names, positions, phone numbers, and addresses are contained in Appendix A. Appendix A identifies management succession if managers are absent or unavailable. Inform them briefly of what has happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. The Emergency Coordinator should inform the executives whether their presence is required and when.
* In activating the Emergency Action Teams, the Team Leaders of each required team will be called from the Notification List in Appendix A. Inform them briefly of what has happened, the current status, the plan of action, and the location and phone numbers of the Emergency Control Center. Each Team Leader has a copy of the Plan and must initiate action appropriate to his/her Team. He or she is responsible for notifying the team to assemble and act according to their recovery plans.

E. Notification of offsite storage and contingency sites

Activation of recovery plans will require retrieval of backups, documentation, and supplies from offsite storage as well as establishing operations at the Contingency Site. Specific Emergency Action Teams, according to procedures identified in this Plan, will carry out these tasks. To expedite the initial recovery process, the Readiness Team will notify both the offsite storage site that a disaster has occurred and that the recovery plans have been activated.

Notifying Procedures For Offsite Storage and Contingency Sites

* Notify the appropriate personnel that offsite storage materials will be required to recover from a disaster. The standing recovery procedures identify what items, (e.g. backup media, supplies, etc.) are to be removed from storage. The procedures also specify precisely what is to be done with the items. The offsite storage location is listed in Appendix B.
* Notify the Contingency Site that a disaster has occurred that requires activation of recovery operations. The Contingency Site is listed in Appendix B.

F. Summary of procedures for recovery operations

This section provides an overview of recovery operations. Summary Of Procedures:

* The Emergency Action Operations Team, or designated members, will go to the offsite storage site and remove the items required by the recovery plans. Because of separate notification by the Readiness Team, the materials are expected to be gathered and ready by their arrival. The Emergency Action Operations Team will verify the materials, making any necessary adjustments, and then assemble at the Emergency Control Center.
* All other activated teams will assemble at the Emergency Control Center for briefing, discussion of any identified problems, and coordination of the recovery plans.
* The Emergency Action Applications Team will proceed to identify the work in progress that needs to be recovered and how that can best be accomplished. They will be responsible for notifying the user departments and coordinating their interface procedures.
* The Emergency Action Operations Team will proceed to the Contingency Site immediately and begin loading software and data to prepare for computer operations. Once established, processing will be maintained at the Contingency Site as long as required.
* If hardware has been destroyed, damaged, or negatively affected, the Emergency Action Hardware Team will proceed to take the appropriate recovery measures to repair or replace the affected hardware.
* If facilities have been destroyed, damaged, or negatively affected, the Emergency Action Facilities Team will proceed to take the appropriate recovery measures to repair or replace the affected facilities.
* The Emergency Coordinator will continue to maintain the Emergency Control Center as long as appropriate, and will coordinate the recovery operations until they can be returned to a normal, non-emergency state.

G. Initial procedures at contingency site

Contingency Site personnel will take the necessary initial steps following our notification that Company has had an emergency and will be using their systems. These procedures include preparations, both general (for them) and unique to our technical system requirements, which they can or need to accomplish before our arrival at their site.

H. Initial procedures at offsite storage site

The following procedures are to be performed by the offsite storage site as the initial steps following our notification that we have had an emergency and require materials from offsite storage.

Procedures At Offsite Storage

* Take the following materials from storage to a staging area for pick up:

The most recent backup media

All backup supplies

All backup documentation

Vendor supplied documentation can be supplied at a later date (if needed)

* DO NOT deliver the materials unless specifically requested. The procedure calls for the Emergency Action Operations Team to go to the storage site, verify that the correct backup materials are being taken, and take the materials with them to the Emergency Control Center. Some materials may be left at the Control Center and some will be taken to the Contingency Site.

I. Pickup of backup materials by emergency action operations team

The following procedures concern the picking up of materials stored off­site.

Procedures For Pickup Of Backup Materials - The Emergency Action Operations Team Leader should arrange for up to two members of the Emergency Action Operations Team to proceed directly to the offsite storage site to pick up all necessary backup materials in one trip. The Emergency Action Operations Team Leader will know from tests or reviews of items in storage how much vehicle capacity is needed. Team members with the appropriate type and size of vehicles (for transportation and protection of materials) will be specified to pick up the materials.

At the storage site, the team members will review the materials for correctness and appropriateness to the requirements of the emergency. See standard emergency items specified in this Plan and the com­plete list of items backed up in offsite storage. If there are problems identified with selected materials, the team members will attempt to select the correct items before dividing the materials into two groups. The materials should be grouped according to destination – Emergency Control Center or Contingency Site - before removal to their vehicles.

Contingency site materials include:

* The backup media
* Supplies
* One set of all documentation

Control Center materials include:

* Supplies for the Emergency Control Center
* Remaining documentation

The team members will proceed to take the materials to the Emergency Control Center. There the Contingency Site materials can be left in the vehicles (locked) and the other materials should be taken in to the Emergency Control Center.

J. Assembling and coordinating of all emergency teams

These procedures address the initial meeting of the Emergency Action Teams with the Emergency Coordinator and other members of the Readiness Team.

Assembling and Coordinating Procedures

* When all the required Action Teams have been assembled at the Emergency Control Center, the Emergency Coordinator will brief the Action Teams on what has occurred and the Readiness Team's assessment of the status.
* Based on this information, all teams will be asked if they are aware of other information or circumstances that need to be considered. The teams should collectively discuss all of the basic aspects of the situation, and considerations of problems due to the processing sched­ule or anything else, before proceeding to carry out their individual team functions. This in important in order that all teams understand all of the key issues. This will result in better coordination.
* Before any teams leave, the Emergency Coordinator will quickly review with each team leader the actions that each team will be taking. Team leader briefings will be done in the following order for the reasons indicated:
* Administrative Assistance - Because the Contingency Site is remote and requires travel, Company management must immediately begin making arrangements for the teams that will be going to the Contingency Site.
* Emergency Action Operations Teams - Needs to proceed to work with the Emergency Action Applications Team concerning work in progress and to coordinate with key users. As soon as those steps are complete, some or all of the team will travel to the Contingency Site.
* Emergency Action Applications Team - Needs to proceed to work with the Emergency Action Operations Team concerning work in progress and to coordinate with key users. As soon as those steps are complete, some or all of the team will travel to the Contingency Site.
* Emergency Action Facilities Team - Needs to proceed to repair or replace the server room as required.
* Emergency Action Hardware Team - Needs to proceed to repair or replace the hardware as required.

K. Activating contingency site by emergency action operations team

These are the procedures for establishing operations at the Contingency Site.

Activating Contingency Site Procedures

* Before proceeding to the Contingency Site, the Emergency Action Operations Team must first coordinate with user departments to determine the status of production files and work in progress. In a case where the combination of work schedule, backup schedule, and offsite storage schedule results in serious loss of data or work already completed, large numbers of users, programmers, and Emergency Action Operations Team members will need to meet to evaluate alternatives. This needs to be accomplished before any of these people leave for the remote Contingency Site. Not all details may be resolved at this meeting because of time considerations. It may be appropriate for the Emergency Action Operations Team to go ahead and leave for the Contingency Site while the Emergency Action Applications Team remains to work with the users.
* Once the issues of lost data or lost work have been resolved to the point that the Emergency Action Operations Team can leave, the Team will prepare to leave for the Contingency Site as soon as possible.
* Upon arrival at the Contingency Site, the Emergency Action Operations Team will first organize all materials (tapes, documentation, hardware and supplies) in an area designated by Contingency Site personnel. For simplicity and control, the materials should not be spread out into many different areas but restricted to a single area if possible.
* Next, the Emergency Action Operations Team should refamiliarize themselves with the facility, the computer operations, and all security procedures to be observed.
* The Team Leader should remind the team members that all activities should setup a special log in addition to the Information Systems Log Form. Make sure everyone understands the importance of complete and accurate logging.
* When Contingency Site personnel have completed their setup prepara­tions, the Emergency Action Operations Team will begin loading data on the hot-site machine. When loading the tapes, the tape drive must be set to 6250 bpi.
* Development files saved on the full backups do not need to be restored, only production software, data, and the operating system.
* If incremental backups since the above last full backup are intact, proceed to restore to appropriate directories. The incremental backups must be restored in chronological sequence.
* After the data, software, and operating system have been restored, the system will may need to be restarted.
* Conduct some simple tests of the applications to verify that the system is operational and working as expected.
* Coordinate with the Emergency Action Applications Team about their specific sequence of steps to recover lost work (data lost due to lost incremental backups and work in progress that was not completed or not backed up). If incremental backups could not be restored, data entered and processed since the last full backup may have been lost and may not be recoverable. However, source documents may be available so that the data can be reentered and reprocessed. If any case, it is the responsibility of the Emergency Action Applications Team to work with the key users to resolve what will be done.
* Once the recovery procedures have been worked out, the recovery work should be carefully scheduled with the Emergency Action Applications Team to ensure that recovery steps happen in a well-controlled sequence. Users will probably need to be present to verify results at each step. The Emergency Action Operations Team and users will probably need to be scheduled in shifts according to the work to be accomplished.
* When the key users have determined that the recovery work has been completed, the resumption of processing can be scheduled. Shift scheduling will need to be continued as appropriate.

L. Recovering lost work by emergency action applications team

The following procedures have been prepared concerning recovery of lost data and work in progress.

Recovering Lost Work Procedures - The Emergency Action Applications Team must coordinate with the users to first identify what work has been lost, if any, through lost incremen­tal backups, lost source documents or other records, and lost work that was in progress and not backed up. Determination of status of all work is the first step that must be accomplished. As much of this process as possible should be done before leaving for the Contingency Site. The Team Leader should notify key users and call a meeting at the Emergency Control Center.

In the case of lost work and lost documents, the Emergency Action Applications Team should work with the users to determine the established plan for recovering the lost documents or the information contained in them. The recovery procedure may allow the lost data to be recovered in some fashion.

If data or work has been lost, the combined teams (Operations, Applica­tions, and Users) must determine how the data or work will be recov­ered. This requires reviewing each application carefully. In cases where data has been lost that is irrecoverable, some decision must be made as to what will be done to account for the lost information. This may mean lost dollars, lost business, or the inability to verify events with auditable records.

Once an action plan has been identified, it may be appropriate for Emergency Action Applications Team members and selected users to travel to the Contingency Site. However, if the recovery process is not difficult and communications are established rapidly, these personnel may be able to do their work remotely via communications links.

The lost work must be recovered as best possible with a combined effort of Operations, Applications, and the Users. This may involve around the clock efforts, doing data entry, correcting data files, running special jobs, or rerunning production jobs. In such a situation, all three groups will need to work in shifts to be scheduled by the Emergency Action Applications Team.

In the recovery process, if there are not enough people to work on all application areas simultaneously, then Company management must be careful to assign the work according to priorities of what is really important, the schedules that are most pressing, and the greatest impacts on the business, particu­larly survivability and profitability.

M. Coordinating users by emergency action applications team

It is the responsibility of the Emergency Action Applications Team to ensure that the applications systems work properly for the users, that lost work is recov­ered, and that the users understand the mode of interface during the recovery operation. The following are the user coordination procedures.

Procedures For Coordinating Users

* Upon completion of the joint disaster review meeting, the Emergency Action Applications Team's first priority is to determine the status of production files and work in progress. They will first coordinate with the Emergency Action Operations Team in this process.
* Depending on time of day, and point of time in the monthly schedule, the Emergency Action Applications Team will probably need to immediately get key users actively involved in the process of determining status. If so, key users will be notified and asked to meet at the Emergency Control Center.
* The Emergency Action Applications Team leader will brief the key users on the initial status situation, then divide employees up into groups by application system or subsystem, preferably with a mix of users, programmers, and operations staff in each group.
* When the issues of recovering most work have been ironed out, the Emergency Action Applications Team leader will coordinate a work schedule with the key users and the Emergency Action Operations Team leader. At this point, impact on ongoing work should be carefully discussed so the key users clearly understand the situation and can give appropriate directions to their subordi­nates. User departments must understand what their interim work plans will be until their automated systems are recovered and back online.
* Once the recovery process is completed, the Emergency Action Applications Team will coordinate with the key users to ensure that they understand how they interface with their applications and what the restrictions are. If the numbers of terminals cannot handle the work load, users will need to work in shifts to take advantage of the available hours. However, the Emergency Action Operations Team leader must be involved in the scheduling to make sure processing conflicts are avoided. If unexpected problems are encountered, the Emergency Action Applications Team will work quickly to find solutions.

N. Hardware salvage or replacing by emergency action hardware team

The following procedures cover hardware salvage or replacement by the Emergency Action Hardware Team.

Hardware Procedures

* Our computer hardware was acquired from equipment vendors identified in Appendix C. In an emergency, our first resource for assessment of damage, repairability, and alternatives is with them. If repair is out of the question, loaner equipment may be immediately available. To speed delivery of new equipment, letters of intent may be on file with selected vendors (see Appendix D).
* In the event equipment can be repaired, Appendix D contains service agreements with ABC Company’s equipment vendors.
* Refer to the Appendix D for all applicable letters of intent. These letters have been approved by Company management and speed delivery of equipment to us during an emergency. Only the final configuration, purchase price, and/or current financing rates will need to be approved at the time of ordering the replacement equipment.

O. Facilities salvage or replacing by emergency action facilities team

These procedures cover salvage or replacement of the network server room facilities under the jurisdiction of the Emergency Action Facilities Team.

Procedures

* To work with Company management to identify options (repair existing or identify replacement) facilities.
* Work with outside vendors as appropriate for environmental, power and repair conditions.

P. Administrative coordinating by administrative team

The Administrative Team will determine the procedures for all administrative assistance regarding hotel arrangements, flight schedules, etc.

Administrative Coordinating Procedures

* Work with Company management to determine extent and duration of resources needed.
* Identify locations and individuals involved.
* Gather and provide the necessary resources.

Q. Specific procedures for user department contingencies

This section contains specific procedures for user interface and operation of their applications. The concept of the Contingency Site Coordinators necessary if a large number of information systems and user department staff must work at a Contin­gency Site.

Procedures For User Department Contingencies - The Contingency Site Coordinator will become familiar with the Contingency Site facility, determine if any aspects are inadequate for the situation at hand, and take necessary action. For example, if the staff accommoda­tion capacity of the Contingency Site is exceeded, the Contingency Site Coordinator is responsible for arranging supplemental facilities. This could happen if an unusually large number of personnel are sent to the Contingency Site because of a disaster that prevents use of the planned communications arrangement. First choice in that particular case would be at the same hotel housing ABC Company’s personnel.

The Contingency Site Coordinator will represent the interests of the company as a whole rather than that of a specific department. He or she will review recovery plans and schedules to ensure that they are in line with the ABC Company’s operations priorities. If there are any doubts, especially if the ABC Company’s operations are affected significantly, the Contingency Site Coordinator will discuss the matter with the Emergency Coordinator who will take the issue to Company management.

During the recovery process and subsequent data processing and adminis­trative operations, the Coordinator will facilitate the teamwork of the multiple departments. He or she will schedule shift work in the best interest of the company, will give pep talks or counseling to keep spirits up, and will be especially alert for team members becoming over stressed.

The Contingency Site Coordinator will stay in regular contact with the Emergen­cy Coordinator to keep him or her current on status, progress, deci­sions made, unusual expenditures, and administrative matters.

R. Operating of application systems

These procedures address operation of the software applications from the Contingency Site.

Procedures For Operating Application Systems - If the planned communications facilities are established successfully, the operations of the business should be as normal except for some reduced numbers of PCs and related equipment. If this causes problems getting all work accomplished, the Emergency Action Applications Team and Emergency Action Operations Teams will assist with supporting staggered shifts so that a fewer number of PCs can handle the load. If other operational problems are encountered, the Emergency Action Applications Team is responsible to find solutions and to coordinate with the users about changes in procedures.

If the planned communications facilities cannot be established at the planned capacity for any reason (e.g. PCs are not operational, software does not run, etc.), the following actions will be taken:

* Heads of user departments will be responsible for sending selected users to the Contingency Site.
* Support of the systems will be accomplished by whatever means are possible, such as E-mail or voice communications to another location, couriers to the main office, etc.
* If branch offices are also unsupported with working PCs and printers, the Emergency Action Operations Team will assist the branch offices and interfacing departments to establish other methods of accomplishing the work, such as use of telephone, express mail, facsimile, etc.
* The key in unusual recovery situations is to be creative rather than panicked.

S. Procedures for replacing network server room

If the network server room is destroyed, steps will be taken immediately to estab­lish a replacement network server room. A location must be found with adequate space; computer rooms must be constructed or modified; and computers, air conditioners, power distribution equipment, cabling, etc., must all be obtained and installed to prepare a working network server room.

Network Server Room Procedures

* The Emergency Action Facilities Team with assistance from the Emergency Action Hardware Team has procedures to identify potential replacement sites and probable means of obtaining equipment and facilities on an emergency basis.
* If equipment or facilities are salvageable, the Emergency Action Hardware Team and the Emergency Action Facilities Teams will assess what is usable or repairable and what needs to be replaced. The Emergency Action Hardware Team will initiate all salvage, relocations, and repair activities as necessary.
* The Emergency Action Hardware Team and the Emergency Action Facilities Team will initiate ordering of all new replacement equipment and facilities on an emergency (rush) basis. Financial, legal, and insurance issues must be considered during this process.
* As the new network server room is constructed and equipment arrives, the Emergency Action Hardware Team and the Emergency Action Facilities Team will coordinate obtaining permits, installation, wiring, etc., to ensure that the network server room is properly prepared.
* The Emergency Action Hardware Team and the Emergency Action Facilities Team will test the readiness of the new network server room. When it is ready, they will coordinate with the Emergency Action Operations Team to transfer operations from the Contingency Site to the new network server room.
* The network server room procedure will be complete when all problems with the new network server room have been resolved and operations have been restored at the new facility.

T. Procedures for returning to normal operations

The following procedures are for returning to normal operations after emergency (recovery) operations.

Returning To Normal Operations Procedures - The Emergency Coordinator must notify company management when information systems are transferred to the original network server room or to a new replacement network server room. As information systems are transferred back to normal operations, the recovery procedure will very quickly be phased down. The Emergency Action Operations Team must leave the Contingency Site with all property and materials belonging to the organization, and use due care and caution to protect all data and software.

The Emergency Coordinator and Readiness Team must main­tain a full state of readiness during, and particularly after, returning to normal operations. The Emergency Action Operations Team will be directed to return materials back to their proper offsite storage, including current backup materials and media.

The Emergency Action Operations Team must inform all users that the emergency or disaster is over and that operations are now or soon to be returned to normal. The Emergency Control Center will be deactivated.

The final activity of the recovery process will be the meeting and debriefing of the Readiness Team, all Coordinators, and Emergency Action Team Leaders concerning the activities of the recovery. The Emergen­cy Coordinator is responsible to make sure that events, problems and solutions, etc., are documented. Once documentation is complete, the Emergency Action Teams and Readiness Team can be deactivated. During the next review of the Plan, the Emergency Coordinator will be responsible to ensure that any lessons learned are incorporated into the Plan.

# XIII. Testing and Maintaining the Plan

After initial acceptance of this Plan, ongoing testing on a periodic basis is necessary to ensure the continued viability of its contents. This Plan must also be reviewed regularly and updated as neces­sary. This section deals with these issues by providing policies and procedures for testing this Plan and for periodic review and update.

A. Policies and procedures for testing

The organization will enforce the following policies and procedures govern­ing testing of the Plan.

Plan Testing Policy - The Plan will be tested for procedural and organizational aspects as well as the technical ability to process information at the Contingency Site referenced in this Plan. Moreover, because it is important for the emergency teams to remain familiar with the recovery procedures, the Emergency Coordinator is responsible for conducting a test at the Contingency Site. The test will be performed each year and the results of the test will be reviewed and approved by Company management.

Plan Testing Procedures - Each year, in conjunction with reviewing and updating this Plan, the Emergency Coordinator must design, schedule and notify team members of the annual test. The test may vary from year to year, in order to evaluate different elements of the Plan, but at the least it must address all major procedures involving all Emergency Action Teams. The tests may be organized as several different tests during the year, each testing a different portion of the Plan.

The tests are to be regarded as review and training exercises as much as tests of the workability of the Plan. However, there will always be some features of the Plan that are truly tested. This means that the tests must be observed, measured, and all successes and failures record­ed. The Alternate Emergency Coordinator will serve as the test monitor. During the progress of the test, if problems are encountered, solutions will be sought at that time.

At least in the initial acceptance tests (first year) and every two   years thereafter, ALL critical applications will be tested to verify that no technical problems prevent those services from working. In intervening years, tests of critical appli­cations may be staggered to reduce the complexity of the tests and the time required.

The tests will extend over a fairly limited time period so as not to have an undue impact on other business activities.

Following the tests, the Emergency Coordinator will document the results of the tests, including any recommended changes in the Plan. The test results will then be reviewed and approved by Company management.

Changes to this Plan, which result from the testing process, will be incorporated along with the changes from the annual review process.

B. Policies and procedures for review and update

The effectiveness of the Plan is impacted by changes in the environment that the Plan was created to protect. Some major factors that impact the Plan are: new equipment, changing software environ­ment, staff and organizational changes, and new or changing applications.

The following policies and procedures have been developed to ensure that the Plan is reviewed and updated on a regular and reliable basis.

Plan Review And Update Policy - Once per year the Plan must be reviewed by the Emergency Coordinator and approved by ABC Company management.

Plan Review And Update Procedures

* The Emergency Coordinator will appoint a review team of one or more people each year to review and update the Plan.
* When the review team has completed their review and update process, the Emergency Coordinator will also review and approve the revised Plan.
* Once approved by the Emergency Coordinator, the revised Plan will be submitted to Company management for final approval.
* The revised Plan (after review and update) will be used as the basis of the annual test. Updates must be distributed prior to the test. However, the tests themselves may also identify changes to the Plan; therefore, final distribution of updates will occur following the tests.
* The Emergency Coordinator will then direct the Alternate Emergency Coordi­nator to distribute the revisions to the Plan. For cost considerations, the revisions will be distributed as updates to the previous version.
* More frequent reviews/updates of the Plan may be initiated by the Emergency Coordinator, but shall require the approval of Company management because of probable impact on other projects.

# XIV. Appendices

Appendix A - Emergency Notification Lists

Emergency Service Numbers

Emergency Readiness Team

Company Management Succession Notification List

Appendix B - Offsite Storage And Contingency Sites

Offsite Storage

Contingency Sites

Emergency Control Centers

Appendix C – Vendor Contacts

Computer Equipment/Services

Communications Equipment/Services

Office Equipment/Services

Appendix D - Service Agreements

Appendix E – Information Systems Equipment Configurations

Computer Equipment

Communications Equipment

Office Equipment

Appendix F – Distribution List For This Document

Appendix G – Summary Of Responsibilities

# Appendix A – Emergency Notification Lists

Description Contact Phone Number

**Emergency Services**

Police, Fire, Ambulance Operator 911

Building maintenance xxx-xxx-xxxx

**Emergency Readiness Team**

Emergency Coordinator xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Alternate Emergency Coordinator xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Contingency Site Coordinator xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Emergency Action Teams

Emergency Action Operations Team xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Emergency Action Applications Team xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Emergency Action Hardware Team xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Emergency Action Facilities Team xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Emergency Action Administrative xxxxxx xxx-xxx-xxxx

Assistance Team Address

City, State Zip

**Company Management Notification Succession List**

Executive xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Finance xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Human Resources xxxxxx xxx-xxx-xxxx

Address

City, State Zip

# Appendix B – Off-site Storage, Sites, Emergency Control Centers

Description Contact Phone Number

**Offsite Storage**

Provider xxxxxx xxx-xxx-xxxx Address  
 City, State Zip  
 Acct #:

The following items reside offsite:

* A copy of this Information Systems Business Continuity Recovery Plan
* Passwords (in a sealed envelope)
* Electronic backup media
* Diskettes
* Technical system documentation (system start up and shut down procedures)
* Blank checks

**Contingency Site(s)**

Location 1 xxxxxx xxx-xxx-xxxx Address  
 City, State Zip

Location 2 xxxxxx xxx-xxx-xxxx Address  
 City, State Zip

Emergency Control Center(s)

Location 1 xxxxxx xxx-xxx-xxxx Address  
 City, State Zip

Location 2 xxxxxx xxx-xxx-xxxx Address  
 City, State Zip

# Appendix C – Vendor Contacts

Description Contact Phone Number

Computer Equipment/Services

Server, PCs, printers xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Acct #:

Industry software xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Acct #:

Communications Equipment/Services

Equipment (Routers, etc.) xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Acct #:

Communications lines (voice) xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Acct #:

Communications lines (data) xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Acct #:

Telephone systems xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Acct #:

Office Equipment/Services

Fax machines xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Acct #:

Copiers xxxxxx xxx-xxx-xxxx

Address

City, State Zip

Acct #:

# Appendix D – Service Agreements

Included In This Appendix

* A copy of the Contingency Site service agreement. (Letter of Intent)
* A copy of the offsite storage facility agreement.
* Copies of all special recovery agreements with vendors, facilities providers, etc.

# Appendix E – Information Systems Equipment Configurations

Computer Equipment Minimum Configuration

Network server minimum configuration:

* Preferred processor XXXXXX
* Hard drive capacity XXXXXX
* Memory (Ram) XXXXXX
* Operating System XXXXXX
* Keyboard, mouse Yes
* Monitor size XXXXXX
* Uninterruptible power supply (UPS) Yes

Workstation system minimum configuration:

* Type (Desktop, Laptop, etc.) XXXXXX
* Hard drive capacity XXXXXX
* Memory (Ram) XXXXXX
* Operating System XXXXXX
* Keyboard, mouse Yes
* Monitor/screen size XXXXXX
* Security/anti-virus XXXXXX
* Productivity suite XXXXXX

Printer minimum configuration:

* Manufacturer XXXXXX
* Minimum 12 pages per minute XXXXXX
* Minimum resolution XXXXXX

Peripheral equipment – not required unless specifically identified below

Communications Equipment Minimum Configuration

Router Manufacturer XXXXXX

Internet Connectivity XXXXXX

Voice lines from telephone provider XXXXXX

Telephone system

* Preferred Manufacturer XXXXXX
* Preferred Model XXXXXX

Office Equipment Minimum Configuration

* + Preferred copier XXXXXX
  + Preferred fax XXXXXX

# Appendix F - Distribution List For This Plan

Position Employee Name

Emergency Coordinator

Alternate Emergency Coordinator

Contingency Site Coordinator

Emergency Action Operations Team Leader

Emergency Action Applications Team Leader

Emergency Action Facilities Team Leader

Emergency Action Admin Assist Team Leader

Offsite Storage

# Appendix G – Summary of Responsibilities

Important locations

* Offsite storage
* Emergency Control Center
* Alternate Emergency Control Center
* Contingency Site

Readiness Team

* Emergency Coordinator
* Alternate Emergency Coordinator
* Contingency Site Coordinator
* Action Team Leaders

Emergency Action Operations Team

Emergency Action Applications Team

Emergency Action Hardware Team

Emergency Action Facilities Team

Emergency Action Administrative Assistance Team

|  |  |  |  |
| --- | --- | --- | --- |
| Emergency Coordinator | Alternate Emergency Coordinator | Contingency Site Coordinator | Emergency Action Operations Team |
| Acts as liaison with fire, police, and remote offices | Implements emergency evacuation plans |  |  |
| Coordinates efforts and directs all activities of Readiness Team | Activates and maintains Emergency Control Center | Activates and maintains Contingency Site | Obtains offsite storage materials and transports to Emergency Control Center and Contingency Site |
| Communicates recovery status to management | Communicates with Contingency Site | Communicates with Emergency Control Center | Initiates recovery efforts at Contingency Site |
| Reviews and oversees updates to Plan | Maintains up-to-date contact information for employees and vendors | Oversees new hardware/software, software updates |  |
| Oversees Plan training | Monitors Plan testing and records progress | Participates in Plan testing | Participates in Plan testing |
|  | Reviews backup procedures |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Emergency Action Applications Team | Emergency Action Hardware Team | Emergency Action Facilities Team | Emergency Action Administrative Assistance Team |
| Coordinates with users | Assesses damage to existing equipment | Assessing initial damages to facilities | Initially notifies employees |
| Assists in identifying data to be recreated | Recommends alternatives to repairing or replacing equipment | Recommends repairing existing offices or locating replacement facilities | Identifies housing and transporting requirements |
| Monitors recovery progress to determine systems are operating correctly | Orders and receives new/loaner equipment |  | Makes appropriate housing and transportation arrangements |
| Participates in Plan testing |  |  | Coordinates with employees |

# Appendix H – Receipt and Acknowledgement

I have read ABC Company’s (Company’s) Business Continuity Disaster Recovery Plan and agree to abide by it as consideration for my continued employment by Company. I understand that violation of the enclosed policies and guidelines may result in disciplinary action including, but not limited to, termination.

This document supersedes all prior electronic equipment policies, guidelines, understandings and representations. I understand that if any of the provisions of this manual are found null, void, or inoperative for any reason, the remaining policies and guidelines will remain in full force and effect.

If I am uncertain about any policy or procedure, I will check with my immediate supervisor or Company management.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_

Employee Signature Date

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Employee Name (Printed)