

CONTINGENCY PLAN OUTLINE

[This example is meant to convey the typical content of a detailed contingency plan. The format will likely vary for each organization. Components may be combined in lists, matrices or charts. Not all components will apply to all healthcare providers.]

I. Initiation

- A.** Work group or team membership and objectives
- B.** Roles and responsibilities for planning, plan approval, and quality assurance
- C.** List of services confirmed as vital
- D.** Strategy and schedule for planning
- E.** Contingency planning processes and protocols
 - 1. Progress reporting
 - 2. Plan review
 - 3. Plan approval
 - 4. Issue resolution process
 - 5. Communication and coordination strategy with relevant intra and inter-agency
- F.** Affirmation of management support
- G.** Assessment of current disaster recovery or emergency preparedness plans
 - 1. (If none exist the Y2K Contingency Plan should drive the creation effort)

II. Business Impact Analysis (Risks)

- A.** Minimum Acceptable Levels of Service
 - 1. List (or matrix) of service dependencies
 - 2. List of service interfaces
 - 3. Commitments to other clients (specific services and service levels)
 - 4. Minimum acceptable levels of service and/or output which could be tolerated under
 - 5. extraneous circumstances
 - 6. List (or matrix) of components critical to support minimum levels of service
 - 7. Executive approval for minimum acceptable service levels
- B.** Failure scenarios (potential risks)
 - 1. Window of vulnerability (time period during which the service may be at risk)
 - 2. Assessment of internal remediation effort status and likelihood to be complete on time

3. Assessment of reliance on, and condition of external services, suppliers and dependencies
 4. (confidence in continued availability of resource)
 5. Potential failure scenarios with likelihood of occurrence
- C.** Impact of each failure scenario on vital business services with likelihood of occurrence
1. List or matrix of impact of each scenario on vital business services with likelihood of occurrence
- D.** Services for which contingency plans will be developed
1. List of services and the scope of contingency required (specific components or systems)
 2. supporting the service that require contingencies)
 3. Executive approval of contingency scope

III. Contingency Planning

- A.** Relevant contingency efforts of local and/or regional partners
- B.** Contingency strategies
1. List of services, components (if applicable), considered contingencies which support them and the benefit of the contingency
 2. Considered contingencies and required resources
 3. Assessment of considered contingencies
- C.** How well the contingency mitigates risks of disruption to service?
- D.** Assessment of time required acquiring, testing and implementing the contingency
- E.** Sustainability of contingency within resource constraints
1. Executive approval for contingency strategies
- F.** Detailed contingency plans (for each contingency)
1. Contingency objective and scope
 2. Contingency triggers
 3. Schedule for preparation and deployment of contingency
 4. Monitoring strategies to ensure identification of triggering events
 5. Roles and responsibilities for contingency preparation and deployment (including updated contacts, contact mechanism and numbers)
 6. Status reporting processes and protocols
 7. Instructions to carry out contingency
 8. Coordination strategy with local and regional healthcare providers (if applicable)
 9. Required resources and estimated costs
 10. Agreements and assumptions with suppliers on whom each contingency is dependent

11. Communications strategy
12. Business resumption strategy

G. Criteria for business resumption

H. Priorities, processes and resources for business resumption

1. Roles and responsibilities
2. When to resume
3. What to resume
4. How to resume
5. Validation/testing strategy for contingencies and business resumption
 - a. Which components will be tested?
 - b. Members of test team(s)
6. Validation/testing plans
 - a. Objectives
 - b. Approach
 - c. Required equipment and resources
 - d. Necessary personnel
 - e. Schedules and locations
 - f. Procedures
 - g. Expected results
 - h. Acceptance criteria
7. Validation/testing results
(Assessment of capability of contingencies and business resumption)
 - a. Adequacy to support vital service
 - b. Capacity to manage, record and track contingency activities
 - c. Adequacy of controls
 - d. Adequacy of resource availability to implement and sustain contingencies
 - e. Adequacy of business resumption activities

APENDIX C: BUSINESS CONTINGENCY POINTS TO PONDER

- ❑ Consider a backup generator
- ❑ Store computer systems in a safe, restricted area
- ❑ Run virus checks on PC's and firewall connections
- ❑ Route cables to avoid single points of failure
- ❑ Change locks and passwords when employees leave the company
- ❑ Negotiate maintenance contracts that guarantee quick response and replacement
- ❑ Use surge suppressors and uninterruptible power supplies (UPSs)
- ❑ Preliminary cleanup, such as packaging water-damaged files and books in reinforced boxes, can lessen damage and business interruption following a disaster.
- ❑ Assess personnel strengths and weaknesses in terms of knowledge, skill, and performance in order to compensate accordingly with skeleton crews.
- ❑ Have all employees compose thorough job descriptions and procedures manuals specific to their responsibilities. Then, test to see if substitute personnel, guided solely by the documentation provided, can fulfill duties.
- ❑ Arrange to consult with employees in their absence, ideally with them being accessible to answer questions at any time. Prepare a communications plan to facilitate emergency contacts.
- ❑ For certain circumstances, arrange for transportation -- either company-supplied or contracted from an outside service -- to shuttle employees to and from work.
- ❑ For efficient decision-making and prompt response with disaster declarations, maintain a clear-cut, functional description of what constitutes a disaster for your business.
- ❑ Determine what the impact of declaring or not declaring a disaster would be on your company. This could include loss of revenue, negative publicity, or even loss of one's business.
- ❑ During a recovery operation, watch for signs of excessive stress and fatigue. Even exceptionally good performers reach a point where they no longer can think clearly and are prone to serious error.

- ❑ Identify "at risk" employees -- those who are deeply affected by traumatic stress. Move them to a safe environment under the care of counselors or friends, and assess the need for professional intervention.
- ❑ Prioritize your company's business applications. Determine which ones the organization simply cannot be without, and which can withstand some downtime without causing lasting damage.
- ❑ Determine who will be involved in a disaster declaration process. Based on the needs of your company, decide whether a committee approach or individual should be designated to make the final call.
- ❑ Be cognizant of how much time your company has to make a disaster declaration decision. Premature or late declarations both can have negative effects on one's business.
- ❑ To prevent equipment and furniture toppling, move heavier items to lower storage shelves; brace racks; secure cabinets and light fixtures, tall furniture, and desktop equipment including computers.
- ❑ Cross-train employees in critical business processes so all personnel can perform multiple job functions when called upon to do so.
- ❑ Institute employee assistance programs (EAPs) and implement succession planning for all levels of personnel.
- ❑ Inventory critical supplies and establish vendor and mutual aid agreements for post-disaster operations.
- ❑ Delineate primary and alternate evacuation routes, and establish a safe personnel assembly area.
- ❑ Identify piping vulnerable to snapping; provide a clearance allowance around these pipes using flexible couplings or flexible piping.
- ❑ When names, phone numbers, equipment, roles, and locations change at your company, make sure plans are updated at that time, and not put off until a scheduled plan review.
- ❑ Conduct background checks of all employees and periodic checks of anyone with access to sensitive information.
- ❑ All employees should be educated on the effects of traumatic stress and in ways to help oneself and others who have been impacted by a crisis.

- ❑ When selecting cellular phones, consider features that may be useful during a crisis: emergency call, dual/multiple number assignment module, and memory and speed dialing.
- ❑ As part of your communications survival strategy, preplan to have local and 800 calls transferred to another number, a blank group of trunks, or to cellular phones after a disaster strikes.
- ❑ For businesses located in two-story buildings or higher, evacuation and search and rescue kits are essential -- to include stretchers, light sticks, goggles, etc.
- ❑ Ensure that everyone – from the owner to the temp answering the phones – knows what's expected of them during a disaster. Secure in that knowledge, people are less likely to panic.
- ❑ Training is key to effective personnel response. Employees are apt to carry out assigned duties correctly if they've had time to review, question, and internalize.
- ❑ Stock appropriate emergency supplies, and ensure that all employees know where to find and how to use them. Identify personnel with first aid, CPR, or other medical/emergency response training.
- ❑ Be sure that your alternate site is not served by the same electrical power grid or communications center as your primary facility.
- ❑ When purchasing emergency supplies, don't buy too much or not enough. Plan on serving the needs of 20 to 30 percent of your workforce for 72 hours.
- ❑ Paper files take up space and can be a fire hazard if stored improperly; throw out piles of paper that are gathering dust to reduce risk.
- ❑ Before fighting a fire in the workplace, be sure that the fire is small enough to be extinguished with a portable extinguisher. Do not attempt to fight a fire that is large or spreading rapidly.
- ❑ Do not pinch electrical cords under or behind furniture; doing so runs the risk of fire.
- ❑ Maintain current, accurate status information on personnel, facilities, and resources. In the event of an emergency, you will need these items close at hand.
- ❑ Identify facilities in your area that could use hazardous materials. Determine whether an incident could affect your facility.
- ❑ Do not overestimate the security features of protective products, such as fireproof safes, window film, and firewalls; doing so could leave you under protected.

- ❑ If your company allows smoking, limit it to designated areas. Supply large tip-proof ashtrays and make sure everything in them is cold before emptied.
- ❑ Leave space for air to circulate around heaters and other heat-generating equipment such as copy machines and computer terminals.
- ❑ If your computer is making an unusual noise, turn it off. There is a good chance it has suffered or will suffer a head crash. The faster it is deactivated, the better the chance for data recovery.
- ❑ In the aftermath of a disaster, provide press releases detailing the "when, where, how, and why" of an incident; keep records of all information released.