<Company>

Business Continuity Plan

By Paul Kirvan, CISA, CSSP, FBCI, CBCP

CLICK HERE FOR THE EDITABLE WORD DOC VERSION

Emergency notification contacts

Name	Address	Home	Mobile phone

Revisions control page

Date	Summary of changes made	Changes made by (Name)

Purpose

The purpose of this business continuity plan is to prepare <Company> in the event of extended service outages caused by factors beyond our control (e.g., natural disasters, man-made events), and to restore services to the widest extent possible in a minimum time frame. All <Company> sites are expected to implement preventive measures whenever possible to minimize operational disruptions and to recover as rapidly as possible when an incident occurs.

The plan identifies vulnerabilities and recommends necessary measures to prevent extended voice communications service outages. It is a plan that encompasses all <Company> system sites and operations facilities.

Scope

The scope of this plan is limited to <describe>. This is a business continuity plan, not a daily problem resolution procedures document.

Plan objectives

- Serves as a guide for the <Company> recovery teams.
- References and points to the location of critical data.
- Provides procedures and resources needed to assist in recovery.
- Identifies vendors and customers that must be notified in the event of a disaster.
- Assists in avoiding confusion experienced during a crisis by documenting, testing and reviewing recovery procedures.
- Identifies alternate sources for supplies, resources and locations.
- Documents storage, safeguarding and retrieval procedures for vital records.

Assumptions

- Key people (team leaders or alternates) will be available following a disaster.
- A national disaster such as nuclear war is beyond the scope of this plan.
- This document and all vital records are stored in a secure off-site location and not only survive the disaster but are accessible immediately following the disaster.
- Each support organization will have its own plan consisting of unique recovery procedures, critical resource information and procedures.

Disaster definition

Any loss of utility service (power, water), connectivity (system sites), or catastrophic event (weather, natural disaster, vandalism) that causes an interruption in the service provided by <Company> operations. The plan identifies vulnerabilities and recommends measures to prevent extended service outages.

Recovery teams

- Emergency management team (EMT)
- Disaster recovery team (DRT)
- IT technical services (IT)

See Appendix A for details on the roles and responsibilities of each team.

Team member responsibilities

- Each team member will designate an alternate
- All of the members should keep an updated calling list of their work team members' work, home, and cell phone numbers both at home and at work.
- All team members should keep this plan for reference at home in case the disaster happens after normal work hours. All team members should familiarize themselves with the contents of this plan.

Instructions for using the business continuity plan

Invoking the plan

This plan becomes effective when a disaster occurs. Normal problem management procedures will initiate the plan, and remain in effect until operations are resumed at the original location or a replacement location and control is returned to the appropriate functional management.

Disaster declaration

The senior management team, with input from the EMT, DRT and IT, is responsible for declaring a disaster and activating the various recovery teams as outlined in this plan.

In a major disaster situation affecting multiple business units, the decision to declare a disaster will be determined by <Company> senior management. The EMT and DRT will respond based on the directives specified by senior management.

Notification

Regardless of the disaster circumstances, or the identity of the person(s) first made aware of the disaster, the EMT and DRT must be activated immediately in the following cases:

- Two or more systems and/or sites are down concurrently for three or more hours
- Five or more systems and/or sites are down concurrently for three or more hours

- Any problem at any system or network facility that would cause either of the above conditions to be present or there is certain indication that either of the conditions are about to occur

External communications

Corporate public relations personnel are designated as the principal contacts with the media (radio, television, and print), regulatory agency, government agencies, and other external organizations following a formal disaster declaration.

Emergency management standards

Data backup policy

Full and incremental backups preserve corporate information assets and should be performed on a regular basis for audit logs and files that are irreplaceable, have a high replacement cost, or are considered critical. Backup media should be stored in a secure, geographically separate location from the original and isolated from environmental hazards.

Department-specific data and document retention policies specify what records must be retained and for how long. All organizations are accountable for carrying out the provisions of the instruction for records in their organization.

IT follows these standards for its data backup and archiving:

Tape retention policy

Backup media is stored at locations that are secure, isolated from environmental hazards, and geographically separate from the location housing the system.

Billing tapes

- Tapes greater than three years old are destroyed every six months.
- Tapes less than three years old must be stored locally off-site.
- The system supervisor is responsible for the transition cycle of tapes.

System image tapes

- A copy of the most current image files must be made at least once per week.
- This backup must be stored offsite.
- The system supervisor is responsible for this activity.

Off-site storage procedures

- Tapes and disks, and other suitable media are stored in environmentally secure facilities.
- Tape or disk rotation occurs on a regular schedule coordinated with the storage vendor.
- Access to backup databases and other data is tested annually.

Emergency management procedures

The following procedures are to be followed by system operations personnel and other designated <Company> personnel in the event of an emergency. Where uncertainty exists, the more reactive action should be followed to provide maximum protection and personnel safety.

Note: Anyone not recognized by the IT staff as normally having business in the area must be challenged by the staff who should then notify security personnel.

These procedures are furnished to <Company> management personnel to take home for reference. Several pages have been included to supply emergency contacts.

In the event of any situation where access to a building housing a system is denied, personnel should report to alternate locations. Primary and secondary locations are listed below.

Alternate locations

Workplace: <Name>

- Attempt to contact your immediate supervisor or management via telephone. Home and cell phone numbers are included in this document

Workplace: <Name>

- Attempt to contact your immediate supervisor or management via telephone. Home and cell phone numbers are included in this document

Workplace:<Name>

- Attempt to contact your immediate supervisor or management via telephone. Home and cell phone numbers are included in this document

In the event of a natural disaster

In the event of a major catastrophe affecting <Company> facility, immediately notify the **<Name or title of person>.**

Procedure

STEP	ACTION
1	Notify EMT and DRT of pending event, if time permits.
2	If the impending natural disaster can be tracked, begin preparation of site within 48 hours as follows: • Deploy portable generators with fuel within 100 miles. • Deploy support personnel, tower crews, and engineering within 100 miles. • Deploy tractor trailers with replacement work space, antennas, power, computers and phones. • Facilities department on standby for replacement shelters • Basic necessities are acquired by support personnel when deployed: • Cash for one week • Food and water for one week • Gasoline and other fuels • Supplies, including chainsaws, batteries, rope, flashlights, medical supplies, etc.
3	24 hours prior to event: • Create an image of the system and files • Back up critical system elements • Verify backup generator fuel status and operation • Create backups of e-mail, file servers, etc. • Fuel vehicles and emergency trailers • Notify senior management

In the event of a fire

If fire or smoke is present in the facility, evaluate the situation, determine the severity, categorize the fire as major or minor and take the appropriate action as defined in this section. Call 9-1-1 as soon as possible if the situation warrants it.

- Personnel are to attempt to extinguish minor fires (e.g., single hardware component or paper fires) using hand-held fire extinguishers located throughout the facility. Any other fire or smoke situation will be handled by qualified building personnel until the local fire department arrives.
- In the event of a major fire, call 9-1-1 and immediately evacuate the area.
- In the event of any emergency situation, system security, site security and personal safety are the major concerns. If possible, the operations supervisor should remain present at the facility until the fire department has arrived.
- In the event of a major catastrophe affecting the facility, immediately notify senior management.

Procedure

STEP	ACTION
1	Dial 9-1-1 to contact the fire department.
2	Immediately notify all other personnel in the facility of the situation and evacuate the area.
3	Alert emergency personnel on: **<PHONE NUMBERS>** Provide them with your name, extension where you can be reached, building and room number, and the nature of the emergency. Follow all instructions given.
4	Alert the EMT and DRT. *Note:* During non-staffed hours, security personnel will notify the Senior Executive responsible for the location directly.
5	Notify Building Security. Local security personnel will establish security at the location and not allow access to the site unless notified by the Senior Executive or his/her designated representative.

6	Contact appropriate vendor personnel to aid in the decision regarding the protection of equipment if time and circumstance permit.
7	All personnel evacuating the facilities will meet at their assigned outside location (assembly point) and follow instructions given by the designed authority. **Under no circumstances may any personnel leave without the consent of supervision.**

In the event of a network services provider outage

In the event of a network service provider outage to any location, the guidelines and procedures in this section are to be followed.

Procedure

STEP	ACTION
1	Notify senior management of outage. Determine cause of outage and timeframe for its recovery.
2	If outage will be greater than one hour, route all calls via alternate services. If it is a major outage and all carriers are down and downtime will be greater than 12 hours, deploy satellite phones, if available.

In the event of a flood or water damage

In the event of a flood or broken water pipe within any computing facilities, the guidelines and procedures in this section are to be followed.

Procedure

STEP	ACTION
1	Assess the situation and determine if outside assistance is needed; if this is the case, dial 9-1-1 immediately.
2	Immediately notify all other personnel in the facility of the situation and be prepared to cease voice operations accordingly.
3	Immediately notify all other personnel in the facility of the situation and be prepared to cease operations accordingly.
4	Water detected below the raised floor may have different causes: • If water is slowly dripping from an air conditioning unit and not endangering equipment, contact repair personnel immediately. • If water is of a major quantity and flooding beneath the floor (water main break), immediately implement power-down procedures. While power-down procedures are in progress, evacuate the area and follow management's instructions.

Plan review and maintenance

This plan must be reviewed semiannually and exercised on an annual basis. The test may be in the form of a walk-through, mock disaster, or component testing. Additionally, with the dynamic environment present within <Company>, it is important to review the listing of personnel and phone numbers contained within the plan regularly.

The hard-copy version of the plan will be stored in a common location where it can be viewed by site personnel and the EMT and DRT. Electronic versions will be available via <Company> network resources as provided by IT. Each recovery team will have its own directory with change management limited to the recovery plan coordinator.

Alert/Verification/Declaration phase (x-x hours)

Plan checklists

Response and recovery checklists and plan flow diagrams are presented in the following two sections. The checklists and flow diagrams may be used by IT members as "quick references" when implementing the plan or for training purposes.

Insert checklists and other relevant procedure documents here.

Plan checklists

Initials	Task to be completed

Flow diagrams

Insert flow diagrams and other relevant procedure documents here.

Notification of incident affecting the site

On-duty personnel responsibilities

If in-hours:

Upon observation or notification of a potentially serious situation during working hours at a system/facility, ensure that personnel on site have enacted standard emergency and evacuation procedures if appropriate and notify the EMT and DRT.

If outside hours:

IT personnel should contact the EMT and DRT.

Provide status to EMT and DRT

Contact EMT and/or DRT and provide the following information when any of the following conditions exist: (See Appendix B for contact list.)

- Two or more facilities are down concurrently for three or more hours.
- Any problem at any system or location that would cause the above condition to be present or there is certain indication that the above condition is about to occur.

The EMT will provide the following information:

- Location of disaster
- Type of disaster (e.g., fire, hurricane, flood)
- Summarize the damage (e.g., minimal, heavy, total destruction)
- Meeting location that is a safe distance from the disaster scene

- An estimated timeframe of when a damage assessment group can enter the facility (if possible)
- The EMT will contact the respective market team leader and report that a disaster involving voice communications has taken place.

The EMT and/or DRT will contact the respective <Company> team leader and report that a disaster has taken place.

Decide course of action

Based on the information obtained, the EMT and/or DRT need to decide how to respond to the event: mobilize IT, repair/rebuild existing site (s) with location staff, or relocate to a new facility.

Inform team members of decision

If a disaster is not declared, the location response team will continue to address and manage the situation through its resolution and provide periodic status updates to the EMT/DRT.

If a disaster is declared, the EMT and/or DRT will notify IT Tech Services immediately for deployment.

Declare a disaster if the situation is not likely to be resolved within predefined time frames. The person who is authorized to declare a disaster must also have at least one backup person who is also authorized to declare a disaster in the event the primary person is unavailable.

Contact general vendors (see Appendix I)

Disaster declared: Mobilize incident response/Technical services teams/Report to command center

Once a disaster is declared, the DRT is mobilized. This team will initiate and coordinate the appropriate recovery actions. Members assemble at the designated location as quickly as possible. See Appendix E for emergency locations.

Conduct detailed damage assessment (This may also be performed prior to declaring a disaster.)

1. Under the direction of local authorities and/or EMT/DRT, assess the damage to the affected location and/or assets. Include vendors/providers of installed equipment to ensure that their expert opinion regarding the condition of the equipment is determined ASAP.

   A. Participate in a briefing on assessment requirements, reviewing:
      (1) Assessment procedures
      (2) Gather requirements
      (3) Safety and security issues

   NOTE: Access to the facility following a fire or potential chemical contamination will likely be denied for 24 hours or longer.

   B. Document assessment results using assessment and evaluation forms contained in Appendix G.

      Building access permitting:
      - Conduct an on-site inspection of affected areas to assess damage to essential hardcopy records (files, manuals, contracts, documentation, etc.) and electronic data.
      - Obtain information regarding damage to the facility (s) (e.g., environmental conditions, physical structure integrity, furniture, and fixtures) from the DRT.

2. Develop a restoration priority list, identifying facilities, vital records and equipment needed for resumption activities that could be operationally restored and retrieved quickly.
3. Recommendations for required resources.

Contact DRT: Decide whether to continue to business recovery phase

The EMT and DRT gather information regarding the event; contacts senior management and provides them with detailed information on status.

Based on the information obtained, senior management decides whether to continue to the business recovery phase of this plan. If the situation does not warrant this action, continue to address the situation at the affected site(s).

Business recovery phase (xx hours - full recovery)

This section documents the steps necessary to activate business recovery plans to support full restoration of systems or facility functionality at an alternate/recovery site that would be used for an extended period of time. Coordinate resources to reconstruct business operations at the temporary/permanent system location, and to deactivate recovery teams upon return to normal business operations.

<Company> system and facility operation requirements

The system and facility configurations for each location are important to re-establish normal operations. A list for each location will be included in Appendix F.

Notify IT staff/Coordinate relocation to new facility

See Appendix A for IT staff associated with a new location being set up as a permanent location (replacement for site).

Secure funding for relocation

Make arrangements in advance with suitable backup location resources. Make arrangements in advance with local banks, credit card companies, hotels, office suppliers, food suppliers and others for emergency support.

Notify EMT and corporate business units of recovery startup

Using the call list in Appendix B, notify the appropriate company personnel. Inform them of any changes to processes or procedures, contact information, hours of operation, etc. (This may be used for media information.)

Operations recovered

Assuming all relevant operations have been recovered to an alternate site, and employees are in place to support operations, the company can declare that it is functioning in a normal manner at the recovery location.

Appendixes

Appendix A: <Company> recovery teams

Emergency management team (EMT)

Note: See Appendix B for contact list. Suggested members to include: senior management, human resources, corporate public relations, legal, IT services, risk management and operations

Charter:

Responsible for overall coordination of the disaster recovery effort; evaluation and determining disaster declaration; and communications with senior management.

Support activities:

The EMT:

- Evaluate which recovery actions should be invoked and activate the recovery teams
- Evaluate damage assessment findings
- Set restoration priority based on the damage assessment reports
- Provide senior management with ongoing status information
- Act as a communication channel to corporate teams and major customers
- Work with vendors and IRT to develop a rebuild/repair schedule

Disaster recovery team

Note: See Appendix B for contact list

Charter:

Responsible for overall coordination of the disaster recovery effort; establishment of the emergency command area; and communications with senior management and the EMT.

Support activities:

- Coordinate with EMT and senior management
- Determine recovery needs
- Establish command center and assembly areas
- Notify all company department heads and advise them to activate their plan(s) if applicable, based upon the disaster situation
- If no disaster is declared, take appropriate action to return to normal operations using regular staff
- Determine if vendors or other teams are needed to assist with detailed damage assessment

- Prepare post-disaster debriefing report
- Coordinate the development of site-specific recovery plans and ensure they are updated semi-annually

IT technical services (IT)

Charter

IT will facilitate technology restoration activities.

Support activities

- Upon notification of disaster declaration, review and provide support as follows:
    1. Facilitate technology recovery and restoration activities, providing guidance on replacement equipment and systems, as required
    2. Coordinate removal of salvageable equipment at disaster site that may be used for alternate site operations

Appendix B: Recovery team contact lists

Emergency management team (EMT)

Name	Address	Home	Mobile/Cell Phone

Disaster recovery team (DRT)

Name	Address	Home	Mobile/Cell Phone

IT technical services

Name	Address	Home	Mobile/Cell Phone

Appendix C: Emergency numbers

First responders, public utility companies, others

Name	Contact Name	Phone

Appendix D: Contact list

Name	Address	Home	Mobile/Cell Phone

Appendix E: Emergency command center (ECC) locations

Emergency command center - <location name>

Primary:	Address Room XXXX City, State Contact: "coordinator of rooms/space - (xxx) xxx-xxxx
Alternate:	Address Room XXX City, State Contact: "coordinator of rooms/space - (xxx) xxx-xxxx

Emergency command center - <location name>

Primary:	Address Room XXXX City, State Contact: "coordinator of rooms/space - (xxx) xxx-xxxx
Alternate:	Address Room XXX City, State Contact: "coordinator of rooms/space - (xxx) xxx-xxxx

Appendix F: Forms

Incident/disaster form

Upon notification of an incident/disaster situation the on-duty personnel will make the initial entries into this form. It will then be forwarded to the ECC, where it will be continually updated. This document will be the running log until the incident/disaster has ended and "normal business" has resumed.

TIME AND DATE

_____

TYPE OF EVENT

_____

_____

_____

_____

_____

LOCATION

_____

_____

BUILDING ACCESS ISSUES

_____

_____

PROJECTED IMPACT TO OPERATIONS

RUNNING LOG (ongoing events)

Critical equipment status form

CRITICAL EQUIPMENT STATUS ASSESSMENT AND EVALUATION FORM

Recovery team: _____

	[----------STATUS---------]		
Equipment	**Condition**	**Salvage**	**Comments**
1. _____	_____	_____	_____
2. _____	_____	_____	_____
3. _____	_____	_____	_____
4. _____	_____	_____	_____
5. _____	_____	_____	_____
6. _____	_____	_____	_____
7. _____	_____	_____	_____
8. _____	_____	_____	_____
9. _____	_____	_____	_____
10. _____	_____	_____	_____
11. _____	_____	_____	_____
12. _____	_____	_____	_____
13. _____	_____	_____	_____
14. _____	_____	_____	_____
15. _____	_____	_____	_____

Legend

Condition:
OK - Undamaged
DBU - Damaged, but usable
DS - Damaged, requires salvage before use
D - Destroyed, requires reconstruction

Appendix G: Building evacuation information

Provide evacuation procedures

Appendix H: Inventory of primary equipment and network services

Provide list of equipment and network services

Appendix I: Inventory of backup equipment and systems

Provide list of equipment

Appendix J: Approved vendor list

Server and computer equipment suppliers

Company Name	Contact	Work	Mobile phone

Communications and network services suppliers

Company Name	Contact	Work	Mobile phone