

THE UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE

# BUSINESS CONTINUITY



## Planning Workbook

PREPARED BY ...  
DEPARTMENT OF ...  
PHONE NUMBER ...

**NOTICE: This document is the property of Judson M. Freed and the University of Minnesota (Copyright® 1998 Regents of the University of Minnesota, all rights reserved). It may be used only by University of North Carolina at Charlotte personnel for the purposes of performing Business Continuity Planning as required by the Chancellor, UNC Charlotte. This document may not be used by any other person or for any other purpose without the express permission of Judson M. Freed and/or the University of Minnesota Department of Emergency Management, B-1 Morrill Hall, 100 Church Street SE, Minneapolis, MN 55455 (612) 625-8047.**

# University of North Carolina at Charlotte

## Business Continuity Planning Workbook

### Purpose

This document is designed to help guide you through the process of drafting a usable business continuity plan.

There are three parts:

First, there is this workbook; then there is a document called the “Planner” – a series of pages meant to provide you with a format for recording all the data you develop. Finally, there is a Compliance Memo. This is a letter that you will submit when your plan is in place.

When you have completed all of the steps in this Workbook, you will have all of the components of a Business Continuity Plan in place. It will then be a simple process to format the document and then print it.

The intent is to develop a usable, working document – not to merely generate another set of papers. Normally, you will only use the BCP once a year, when you exercise it. However, if you aren’t so lucky, you will need something that will actually help you recover your operations following a disaster.

### Definitions

- **“Business Continuity Plan” (BCP)** – A working document that addresses the people, resources, and actions necessary to recover and restore your critical operations/processes following a disaster.
- **“Disaster”** – An unplanned, calamitous disruption of normal operations for a specified period of time. The time will vary depending on the level of criticality of disrupted operation(s).
- **“Planner”** – The companion document to this workbook. It is a series of pages that you can use to record the data you develop during the planning process outlined in this workbook.
- **“Unit”** – Any operating unit or academic department of the University.

## How Long Will This Take?

Depending on the size of your Unit, and the number of critical processes for which you are responsible, developing a plan for the first time may take anywhere from a few weeks to a few months. Four weeks is a recommended average.

### Rationale:

Disaster is not a matter of size. A theft of your office computer may be a disaster, as might be the death of a critical employee. You need to be able to continue to operate in the face of these situations, while the rest of the University continues business as usual. On the other hand, a disaster may encompass the entire University, community, state or nation.

If a fire breaks out in a building on campus and damages only one small office, it's not a big deal –unless it's *your office!* Business Continuity Planning is just what it sounds like – planning *to continue to operate* in the face of an emergency or disaster or interruption – whatever you may call it – and planning a way *to get back to normal operation* as soon as possible after the disaster is over.

Homeowners in flood plains do this every year when the river starts to rise. They buy flood insurance. They check their sump pumps. They fill up sandbags. They move belongings too large to take with them to the upper floors, and they take what they need to survive with them when they go. This is real continuity planning in action.

On April 19, 1995, a federal office building in Oklahoma City, OK was completely destroyed by a bomb. We are all too aware of the physical and emotional toll this tragedy had on the people in that building and on their families. You can easily understand the hardships that were endured to get those damaged federal agencies back up and running.

You may not have thought about the hundreds of other businesses that were damaged by the blast, or were just in the immediate area of the damage. Every one of those businesses was treated as a crime scene and for weeks no one could get into them, even for a minute. Many of those businesses never reopened because they could not continue to operate. Those people lost their jobs and no one knows what long-term impact that economic loss will have on those families in that city.

What would you do if you were told that, even though your office was undamaged, you would not be allowed in for any reason for the next six weeks? With a good Business Continuity Plan in place, and after a little practice in the use of the plan, the answer will be clear – you'd set up operations somewhere else and your unit would continue to function. The conditions may not be ideal, and you wouldn't have all of the tools at your disposal, but you would be able to continue those processes that are critical to accomplishment of your unit's mission.

## **Assumptions and Planning Parameters**

1. The three primary mission requirements of the University of North Carolina at Charlotte are: Teaching, Research, and Providing Services.
2. The highest priority in responding to any disaster is protection of the lives, safety and health of people (students, faculty, staff, vendors, contractors, visitors).
3. The University will attempt to recover and continue operations in the shortest possible time following a disaster in order to fulfill its 3 primary mission requirements.
4. The Critical Business Processes supporting the 3 primary mission requirements (and their Recovery Times outlined on the attached chart) are valid.
5. Any University operation with a Recovery Time Objective greater than 30 days is not critical to supporting the 3 primary mission requirements.
6. Risks to disruption of critical University operations are:
  - a. Loss of people (faculty, staff, students).
  - b. Loss of facilities (buildings, classrooms, labs, studios, housing, offices).
  - c. Loss of infrastructure (utilities, HVAC, telecommunications, data, information technology systems).
  - d. Loss of critical functions and processes (e.g., scheduling, payroll, financial aid, records administration, food services, purchasing).
7. Continuing operations in alternative modes following a disaster will cost more than normal operations.
8. The University is currently under-funded by the state for normal operations.
9. State resources will continue to be constrained. Emergency operating (or recovery) funds from state sources will be limited, particularly in a widespread disaster.
10. Outsourcing supporting operations to the private sector may be less costly than continuing “in-house” operations (e.g., finance, administration, housekeeping, grounds maintenance).
11. An option for continuing University operations may be to suspend (or discontinue) non-critical operations in order to conserve funds to sustain critical operations.
12. The terminal point for any University operation will be when it is no longer possible or affordable to continue that operation in any mode.

# I. Steps for Developing a Business Continuity Plan

## A. Determining Persons in Charge, Mission and conducting a Needs Assessment

1. Identify the name of your Unit, the Unit Manager and the Business Continuity Coordinator. Enter their names in Section I of the “Planner”.
2. Write a mission statement – this basically will be a statement of “what your Unit does”:
  - a) If you don’t already have one, a mission statement can take a long time to develop, and should be an effort of a group of people within your unit.
  - b) Enter the Mission Statement in Section I of the “Planner”.
3. Now, determine if your mission (or a part of it) is critical to the University as a whole. There are three primary mission requirements for the University: Teaching, Research, and Service (to the University or the community).
  - a) If your unit does not conduct (or provide direct support to) one of these requirements, then you don’t need to go farther. Simply complete the Compliance Memo (see the end of this document) and indicate that you do not perform critical functions.
  - b) If your unit conducts or provides direct support to the three primary requirements of the University, you must continue with the planning process. (Critical processes shown on the chart at Appendix D of the Planner must have a BCP).
4. Needs Assessment
  - a) In Section I of the “Planner”, write down the following:
    - (1) Every function (manual or automated) your unit performs.
      - A function may be a transaction (financial or data) or it may be a task, process, or the provision of a service or a piece of equipment.
    - (2) Don’t forget to include routine things such as clerical, data entry, word processing, filing, etc.
      - One way to do this is to identify all your employees and their job descriptions. You need to know the tasks and processes they perform in order to plan for their continuation after a disaster.

(b) Now, identify which, if any, of the tasks and processes you identified are critical (essential) to the ability of your unit to accomplish its mission.

- These are your “Critical Business Processes”
- Critical Business Processes are the main focus of the planning process. The intent of a BCP is to carry out those critical business processes during the disaster, and then to recover the remainder of your functions after the disaster is over. (Keep in mind that it may take a long time to completely recover from a disaster.)

## **B. Risk Assessment**

1. Consider the acceptability of the loss of (or loss of access to) an asset or function, regardless of the cause of the loss. It may be your office, key personnel, an important function (like payroll), or a necessary utility (e.g., electricity, phone, water). Plan for the simple loss of the asset (or function) and not for the cause of the loss. This is called “all hazard planning”. Your assessment should be based on the acceptability of loss of the asset (or function) to your mission accomplishment. In other terms, how long could you do without that asset (or function) before your unit would be ineffective in accomplishing its mission.

2. However, by identifying specific threats and risks, you can take steps now to minimize those specific things which pose the greatest problem.

- A way to assess your specific risks is to use this formula:

Risk Factor = Threat (or cause) X Probability of occurrence

Risk Factor = Fire X 5% = **.05**

Loss Exposure = Risk Factor X Value of Lost Asset

Loss Exposure = .05 X \$1MM (value of lost lab equipment) = \$50,000.

- Those assets with the highest loss exposure and/or highest risk factor are the ones that you should consider first in your planning.

- You can reduce the risk factor to some extent by installing “controls” to minimize the impact of a specific threat. For example: you can install battery backups (or UPS) on your PCs to prevent loss of data due to a sudden power outage. They won’t prevent the power outage, but they will allow your PCs to continue operating for a period of time that will enable you to save your work and shut down without losing any data on your PC. This could result in a significant reduction in Loss Exposure due to this threat.

3. Definitions:

- a) Threat – The cause of a disaster. It may be natural (flood, hurricane, lightning) or man-made (accidental, or intentional), such as operator error, vehicle accident, hacker intrusion, or terrorist attack.

- b) Risk – The effect of the disaster, or a specific loss. This could be loss of a building (or part of a building), loss of utilities (water, electricity, gas), loss of data network or phone system, loss of people, or loss of critical business functions (e.g., registration for classes).
- c) Loss Exposure – The value (quantitative or qualitative) of the asset (or function) times the risk factor.
- d) Controls – Preventive measures. Steps to minimize the risk and/or mitigate the damage caused by the threat.

- Example:

- a) Threat = Fire
- b) Risk = Loss of hard copy files, data disks, and PCs necessary for your unit to accomplish its mission.
- c) Vulnerability = There are no sprinklers in your office. A fire would damage all hard copy files, data disks, and PCs (particulate from smoke will damage these items, even if they are not consumed by flames).
- d) Control = Take steps to remove items that may lead to a fire in your office (extension cords, ungrounded outlets, coffee maker). Have portable fire extinguisher readily available. Install grounded outlets. Secure a contract with a reputable firm for servicing smoke-damaged computer equipment.

- **IMPORTANT !! Remember** that a problem that impacts a vendor or provider of a service to you may cause you to experience a disaster. (Example: failure of the University's mainframes may mean that your functions can't be accomplished for up to 96 hours.)

- a) These are referred to as “interdependencies”, i.e., you depend on someone else's unit, systems, or functions in order to accomplish your mission.
- b) Certain that you consider these interdependencies as possible risks in your Risk Assessment.

#### 4. Steps:

- a) Walk through all areas of your unit. Write down visible threats and things that could trigger them (fire hazards, sprinklers over computers, crowded aisles, broken locks, sensitive documents unsecured, etc.). Don't forget that theft and vandalism are threats, too. Consider other threats that you may not be able to prevent or defend against – weather, death, and off-duty injury of vital personnel. Record these in Section II of the Planner under Threats. As a minimum, address threats that pose these risks: Loss of your facility (building or office), loss of key personnel, loss of critical supporting functions or processes, loss of infrastructure (gas, water, electricity, phone, data network, HVAC, internet connection).

- b) Identify vulnerabilities posed by each threat and record these under the Section II of the Planner under Vulnerability. You might decide that for some threat (e.g., a snowstorm that closes the University for several days), you have no vulnerability - your unit can be down for a couple of days and there's no harm done. So, you don't need to put a high priority on planning for this. Record each Vulnerability on a scale of 0 to 5.
- c) For each item discovered in section a) for which a vulnerability exists in your unit, identify feasible controls. List these in Section II of the planner under Feasible Controls.

**Example:** You discover that you face a loss of your files (risk) from fire (threat). Since a fire would also set off sprinklers that are located over your computers, you also face a loss of your computer hardware (another risk). You also find things that could trigger a fire (overloaded receptacle, with coffee pot, hot plate, and printer plugged into the same ungrounded receptacle). To reduce your vulnerability, you might remove the hot plate and coffee maker from the receptacle, since they are not mission essential equipment. You could also move the computers to a less vulnerable location in the office. Or, you could install controls that would further reduce the threat (have grounded receptacles installed, put protective canopies over the computers, replace file cabinets with fireproof versions).

<b>Risk</b>	<b>Threat</b>	<b>Vulnerability (Scale of 0 to 5 where 0 = negligible and 5 = high)</b>	<b>Feasible controls</b>
<b>Loss of files</b>	<b>Fire</b>	<b>4 (High)</b>	<b>Install grounded receptacles</b>
<b>Loss of computer hardware</b>	<b>Sprinkler/water damage</b>	<b>5 (High)</b>	<b>Install protective canopies</b>

Note: Feasible and affordable are not always the same thing. However, loss is often far more costly than installing controls.

### **C. Preventive Measures**

- a) Now, carry out the feasible controls you have identified in the preceding steps. Implement the process necessary for installing the controls you have identified. If the risk can be eliminated or reduced by simple measures, do so. Once you have reduced your vulnerability to as many risks as you can with simple solutions, re-evaluate your unit's work areas for remaining risks, threats, vulnerabilities, and controls.
- b) The items that are your primary concern are those with the highest vulnerability remaining and/or those over which you have little or no control. However, you will have significantly reduced the impact of a disaster on your unit.

- c) Create a plan for evacuation of your unit in the event of a fire or similar emergency during business hours. Be sure to include a place for personnel to meet, so you can be sure that they are safely out of the building. Establish this point at a safe location away from your building (and others that may also be affected by a larger scale emergency). Special consideration should be given to physically disabled individuals who may need assistance in evacuating (elevators will not normally be used for evacuation). And, you may need special procedures to secure data and/or equipment. The first priority, though, is always people. Record your evacuation plan in Section II of the Planner, and be sure to disseminate it to your entire staff. For assistance with developing an evacuation plan, contact the Department of Environmental/Occupational Safety and Health at x4291.

## D. Mission Impact Analysis

What will be the impact of disruption of your operations over time, without consideration of the cause of the disruption?

This is a qualifier for your Risk Assessment. Here, you simply consider that, if for any reason you cannot use something or do something, it will impact on your mission.

Since there are an infinite number of *possible* disasters and a large number of reasonably *likely* disasters, no one can list all of them – much less plan for every one. So, we ask you to simply assume that for *some reason* you cannot access what you need. You determine the time frame for which such a disruption is acceptable. (This time can also be driven by someone else who depends on your function to accomplish their mission. These are called “interdependencies”.) Some of the obvious critical functions of the University have already been identified and Recovery Time Objectives have been established for them (see Appendix). If your unit is responsible for one of these functions, or that function depends on your unit’s being able to do its job, then the maximum acceptable time is already established. Your unit must be able to function at least at a minimal level by that time. Recovery to normal operating levels may take longer.

1. In section I of the Planner you have listed your Mission Critical functions in three categories:
  - Teaching
  - Research
  - Providing a Service
- b) Copy each function described in Section I of the Planner as “critical” into Section III of the Planner. List all personnel (by name and title, or position) and list all equipment or supplies you need to perform that task or carry out that process.
- c) For each critical function listed in Section III of the Planner, consider what would happen to your operating unit, if you could not perform that function.

## 2. Time to Failure

- a) Identify how long your unit can carry out its mission without doing each function you described in Section III of the Planner. This is your Recovery Time Objective. If you can't be back in operation within that time, your unit will not be able to accomplish its mission.
- b) You now know how long you can take to get your plan activated and operational. This tells you how long (hours, days, minutes) you can take to activate your plan, notify the right people, bring in new equipment, buy replacement supplies, etc. If your plan works, you will have all of the equipment and supplies you need to provide a minimum level of operation to meet your mission requirements.

## 3. Determine Minimum Level of Operations – **You will need to generate more data in other parts of this workbook in order to complete this step. Do what you can now, and fill in the other information as directed.**

- a) Determine the minimum personnel, supplies, equipment, etc. your unit needs to meet its mission requirements. It could be that your sophisticated Voice Mail system is a great convenience for you and your team. During an emergency that system may not work. Is it “critical”, or could you operate with an answering machine for a few days or weeks? Be brutal in this assessment. You are not saying that you can perform your tasks at this level indefinitely. However, reaching an understanding of the bare minimums at which you can function temporarily is an imperative portion of your planning process.

### Example:

Does everyone in your office need a separate computer all of the time? For normal operations, that makes life easier, but during a disaster could a couple of staff members share one? Perhaps your staff could work shifts in order to share time on a single computer. You couldn't do this every day, and the people you serve might not want you to. But during a disaster you might be able to use such a scheme to allow three people to work full time (avoiding loss of pay or layoffs), get all of your processes completed, and only need to replace one computer.

- b) First, document a time line that starts with the disaster.
- c) Second, consider how long you can take to make the decision that this is a disaster. (If you and your staff can't decide within this time frame, then err on the side of caution and declare the event a disaster).
- d) Third, indicate how long you can allow for notification of appropriate persons. Estimate how long it will take to gather your Recovery Team together.
- e) Fourth, consider how long it will take to set up at your alternate work site (if applicable) or to begin work again at your current site – and how long it will take to get “up and running”.

- f) Fifth, identify the minimum level of operation you intend to offer to meet the critical functions you have identified. **Exclude all non-critical functions and processes.** This is not *business as usual* and you cannot do everything you would normally do, no matter how much you may want to. Remember that this is a *temporary* situation.
  - g) Now, describe the tasks and processes you will and will not provide during the disaster in Section III of the Planner. This is your Minimum Level of Operation. Everyone in your Operating Unit needs to know, understand *and accept* these for what they are – a temporary means of making sure that the critical missions you provide continue to be carried out.
  - h) It is advisable to seek input from the various personnel affected.
4. You should revise this recovery time line as needed during the remainder of the planning process and during all revisions to the plan.

## **E. Identify a Recovery Team**

In Section IV of the Planner, identify the following personnel. List the name of each person and an alternate. Include home, office, and cell phone or pager numbers. These people are the recovery operations staff. Among these:

1. Decide who can declare that this incident is a disaster (for your Operating Unit).
2. Determine who will be involved in decision-making for the time it takes to get things set up. This will not be your entire staff, but will be only those with immediate recovery responsibility. Establish a chain of command. Someone must be in charge. You need to spell out who has authority to act until more senior people arrive and take control.
3. Determine who will be responsible for getting the word out to all staff members.
4. Assign Personnel.
  - a) You will need (depending on the size of your Operating Unit and the scope of your plan) either a person or a team to handle recovery operations. This team must include personnel who will interface with University-wide response efforts if the disaster is large enough that the University activates its Emergency Operations Plan.

**One person can fill more than one functional role.** The idea is to make sure that *someone* is carrying out each function.

Your Operating Unit may decide to assign a team to each function, or have one person carry out that role. In any case, keep teams small. One person should supervise no more than 5 to 7 others during a disaster.

- Management – People who coordinate responses and provide oversight during an event. People who **may** declare a disaster. People who work to develop your Plan. A member of this team might also represent your Operating Unit at the College, Division, or University level Emergency Operations Center.
- Administration and Logistics – People who coordinate all support functions (which may include child care, transportation, etc.) during a disaster. If they are to leave their home to respond to a disaster, people must be assured that their own families are safe and secure.
- Liaison – Answer phones and provide information to the Communications Team. Work with other affected Operating Units – particularly important when you have interdependent functions with other Operating Units.
- Communications – Provide a single point of contact for information regarding the disaster and recovery process to staff, faculty, and students – and to the University administration.

**Note:** Contact with media should be coordinated through the University Relations office, 2<sup>nd</sup> Floor Reese Bldg, (704) 687-2143, (704) 687-6379.

- Restoration / Security – Ensure that sensitive processes, data, etc. are protected during the disaster and recovery. Oversight of recovery and reinstallation of these items.
- Software / Systems – Specify and obtain hardware and software needed to carry out critical functions. Pick up and install equipment and backup copies of software and data files during the recovery (these people will physically go to the off-site storage locations to retrieve backup items).

b) In addition to the above functions, you should also plan for the following functions:

- Disaster Site Group – People who will deal with and report on the emergency by going to the site. (These people may also serve as technical experts to the emergency responders, if required).
- Recovery Site Group – These people will establish and maintain operations at an alternate location, if needed. If you cannot quickly return to your normal facility/office, this team will be charged with going to the alternate site, setting it up so your Operating Unit can begin functioning again as soon as possible.
- Salvage and Procurement Group – These should be experts who will evaluate damage, salvage equipment, and get it to a repair center. They will need an up-to-date resource list and a list of what needs replacing. They will be charged with taking action to procure new equipment and supplies, and should be involved with setting up back-up agreements and contracts. They may also be people from vendors, Service

Bureaus, or other Operating Units with whom you have pre-arranged agreements. (Copies of these agreements should be placed in *Appendix A* (for UNC Charlotte Operating Units) or *Appendix B* (for non-UNC Charlotte vendors or Service Bureaus).

- Mitigation Group – Members of your Management Group who will work to implement the preventive measures outlined in Section II of the Planner – before a disaster – and who will be tasked with incorporating risk reduction measures into your Operating Unit as it recovers from a disaster so as to reduce risk in the future.
- c) People should be assigned to teams by name and position / job title. This is done so that new employees can be plugged into the plan without much effort. By having the list by job title, it is easy for new people to see where they fit into the team structure.
- d) Don't forget to assign backup personnel. Someone will always be on vacation, maternity leave, or out sick.
- e) Assign an alternate team leader for each group.
- f) Base the teams on your Operating Unit's current organizational structure as much as possible.
- g) Consider making up team "Action Plans". These are concise, easy to follow checklists that tell team members what they need to do. They serve to ensure that all of the essential requirements of the team are met. For instance:

**EMERGENCY ACTION PLAN FOR MANAGEMENT TEAM**

- Call Team Leaders for all teams.
- Call Vice Chancellor – inform of situation.
- Call Acme Offsite Storage to arrange for access by Software / Systems Team
- Call Ajax Room Rentals and procure meeting room (see contract #A172, attached)
- Call phone company to arrange to forward calls to new numbers at Ajax Room Rental location.

- h) Record keeping is an imperative. The number one cause for lost litigation and refusal of insurance claims is poor documentation. A check list with times, dates, actions and initials demonstrates precisely what you did and when.

Attach copies of these checklists to each Team description in Section IV of the Planner.

- i) Cross train. Be sure that people can accomplish the tasks of other teams.

## **F. Identify Lost Resources and Information.**

1. In Section V of the Planner, indicate how you will identify lost resources and information. This might be a checklist or some other means of identification. Use the list of functions in Sections I and III of the Planner to guide you.
2. Start with the critical functions and then go on to the others. What you find during this part of the planning process may cause you to go back and redefine your time to failure, minimum operations levels, and recovery time line. That is why this is one of the last steps. This procedure serves as a review and check on what you have done so far.
3. Once you know what you've lost, you must identify how you'll get those resources back. You will plan out this process in the next step.

## **II. Recovery Strategy**

**Note:** You may choose to plot a recovery strategy for each type of interruption or just in general. However, as you cannot possibly plan for every possible problem, it is usually best to plan for generalities.

For purposes of this plan, consider the following risks (losses): Loss of your facility (office, building, classroom, lab), loss of people (faculty, staff, students), loss of infrastructure (utilities, phone, data network, Internet), loss of functions (systems or processes that you rely on to get your job done – like FRS, SIS, HRIS).

### **A. Determine Your Needs**

1. Refer back to the list of your Mission Critical Functions in Section III of the Planner (Strategic Needs).
  - a) Copy the list of required equipment, forms, processes, etc. from that section into Section VI of the Planner.
  - b) Back up these files using a method appropriate to the type of media.

- (1) Store the back-ups in an off-site location, appropriate to the media type. List the location and the name and phone numbers of the contact for the storage location in Section VI of the Planner.
- (2) On the same page, indicate which persons are authorized access to the off-site storage locations.

**NOTE:** The storage site should offer 24 x 7 access to any files necessary for carrying out day-to-day or emergency operations. However, your Operating Unit may have records or data that are required (e.g., by law) to be available, but are not needed on a day-to-day basis. These files do not need to be available 24 x 7.

2. Determine interdependencies.

- a) Does the function require that something else must occur first? (E.g., for the function “deposit checks from students”, you must first receive the checks, and in order to receive them, you must send out invoices.)
- b) Determine Service Bureaus, vendors, or other Operating Units (e.g., in order to send out the invoices, you need addresses from the SIS).
- c) Determine necessary office equipment, software and supplies. (E.g., to print the invoices, you need a PC, a printer, and the database software on which you have the records. You also need the invoice forms.) **Important:** Be sure to plan for a supply of necessary paper forms to be used in a disaster.
- d) Determine needs for performing the function. (e.g., to print out the invoices, you need electricity, office space and a person).
- e) List these interdependencies in Section VII of the Planner.
- f) Example:

<b>Process / Function</b>	<b>Steps to Carry Out</b>	<b>Interdependencies</b>
Issue Transcript	<ol style="list-style-type: none"> <li>1. Receive request</li> <li>2. Verify attendance/credits</li> <li>3. Print transcript</li> <li>4. Verify transcript</li> <li>5. Address label</li> <li>6. Mail transcript</li> </ol>	<ul style="list-style-type: none"> <li>- Mail delivery services</li> <li>- PC / Network / SIS</li> <li>- Official Transcript Form</li> <li>- Signature / raised seal</li> <li>- PC / Printer / Electricity / Admin Assistant.</li> <li>- Mail services / postage meter</li> </ul>

3. Now that you are aware of what is needed to continue to provide your function, you must develop a means of providing for that continuation.

- a) Contact the Operating Unit(s) providing functions necessary to your process / function.
  - (1) Develop a back-up agreement with that Unit, or identify a different source from which you can get the necessary equipment, process, software application, or people to carry out your process / function. In the example above, the SIS is not available from other sources, but the PC, printer, and admin assistant could be.
  - (2) Attach agreements with UNC Charlotte Operating Units to Appendix A of the Planner, and agreements with non-UNC Charlotte vendors and/or services to Appendix B of the Planner.
- b) For any non-UNC Charlotte vendor or service, you should secure written verification that they have a Business Continuity Plan. Agreements with vendors or services that do not have a Business Continuity Plan (a.k.a., “Operational Continuity Plan”, “Disaster Recovery Plan”) do not afford you any assurance that they will be there when you need them.

## **B. Prioritize**

1. In Section III of the Planner you identified your Mission Critical Functions. Now, go back to that Section and identify to which category (Teaching, Research, Provide Service) each of these functions belongs.
2. Remember that, while all of these functions are critical, some need to be “up and running” sooner than others and are in fact interdependencies.
  - a) Review the previous section. Be sure that you have identified the steps needed for all critical processes. This will enable you to determine which things need to happen first.
  - b) NOTE: It is imperative that you contact any other University Operating Unit or any service that is provided to you that you need in order to meet your minimum level of operations. You and that Unit / service must agree on what will be done on what level. DO NOT ASSUME that another Unit / service will provide anything during a disaster, unless you confirm that their support will be available (and when). Failure to do this is the single biggest mistake you can make in the planning process.
3. Prioritize things you can arrange or correct without outside help. For example, don’t assume that the telephone system will be operational in a disaster situation. You can, however, pre-arrange for temporary use of cell phones and/or radios. This means you can still maintain voice communications until the main phone system is operational.
4. Now, prioritize the other steps that need to be taken (by other Units/services).
5. List these priorities in Section VIII of the Planner.

## C. Return to Normal Operations

1. The minimum levels of operation you indicated in Section III of the Planner are a stopgap. Now, you should give some thought to how long it will take for you to “ramp up” from the minimum operational levels to your normal level of operation. Use the last part of the Planner (Section VIII) for this.
  - a) Consider the idea that you cannot get into your current offices or lab space to retrieve anything. Do not worry about why this is so.
    - If your current work space is destroyed or can’t be occupied for several months, how long will reconstruction take? How long will it take to work through leasing arrangements for a fully-equipped space?
  - b) Outline the order in which you will recover, reactivate, or again provide full services, processes and/or functions.
    - (1) Develop at least two time lines:
      - (a) Long-term or permanent relocation (and/or reconstruction of your current work space).
        - (i) Procure and install all office equipment, hardware, software, data, and supplies not covered by minimum operating levels.
        - (ii) Update all records, processes, etc., at the new site to ensure that they match what has been going on under your minimum operating levels.
        - (iii) Move all personnel into new office space.
      - (b) Move back into current work space.
        - (i) Procure and install all office equipment, hardware, software, data and supplies, not covered by minimum operating levels.
        - (ii) Test, repair and/or replace all hardware that might have been damaged during the emergency.
        - (iii) Update all records, processes, etc. at the site to ensure that they match what has been going on under minimum operations.
        - (iv) Move all staff personnel back into the work space.

(2) You will again need to contact other Operating Units or services upon whom you rely to make sure that they agree with your time lines and assumptions. Indicate which parts of the time lines are actual numbers, and which are estimates.

c) In Section VIII of the Planner, indicate your best estimates regarding the times and sequence of returning to “normal” operating levels.

## **D. Implementation**

1. In Section IX of the Planner, write out what steps need to be taken to activate your plan and notify personnel. These steps should include:

- a) Recognition of the problem (how will anyone know that something has gone wrong?).
- b) Declaration of emergency/disaster.
- c) Notification of staff.
- d) Evacuation of offices, classrooms, labs (if necessary).
- e) Meeting place for personnel (if evacuation is necessary).
- f) Other Units/services and/or vendors that must be notified.
- g) Time line of other Unit/service and/or vendor to accomplish your needs.
- h) Source of replacement of paper goods/office supplies (if necessary).
- i) Source of replacement office equipment, hardware.

2. These items must be pre-arranged and should be in writing. Include copies of all written agreements with other Units/services and/or vendors in Appendices A and B of the Planner.

3. Establish two gathering points for your staff.

- Where to meet if you should have to evacuate during office hours (usually the entire staff of your Unit should meet there to ensure that everyone is safe).
- Where to meet if the emergency occurs during other than normal office hours – and who should go there.

4. Establish an Emergency Operations Center (EOC) at the University, College and/or Division level.

- a) This should be a facility from which your Recovery Team will operate during the disaster.
- b) The EOC may be a pre-designated room or location, but you should have an alternate location in case the primary site cannot be used. You may choose to conclude an agreement with a hotel or some other off-campus location to provide you with this space in an emergency.

- c) The EOC should have some basic items “pre-positioned” for use. At a minimum, a copy of your Plan and up-to-date phone numbers must be available.
  - d) The University has an EOC designated for use in large-scale, long-term situations. And, there are several alternate locations both on and off-campus. For further information, contact the office of Business Continuity Planning at (704) 687-2740.
5. Establish a temporary site from which you can function. Students and staff may have to come to you, so have a place for them to go (this site can be off-campus).
  6. Refer back to Section IV (Recovery Teams) of the Planner. List the titles, names and contact numbers of all other persons with a formal role in the recovery process who have not been listed elsewhere. Explain their roles.
  7. In Appendix C of the Planner, list the names of all persons with copies of your plan. Also, indicate the location of any off-site copies. This is done so that, when you make changes to the plan, you can be sure that all copies of the plan are brought up to date.
    - Each time you distribute changes to the plan, be sure to have all persons who have copies, sign for receipt of those changes. This procedure will ensure that everyone has the latest information at all times.

## **E. Contact Procedures**

- Draw up a procedure for contacting first the operations staff personnel listed in Section IV of the Planner, and then any other appropriate University Units/services, vendors. This will mean maintaining a copy of a contact list in your Plan. Record this in Section IX of the Planner.

## **F. Resource List**

1. In Section X of the Planner, list all Units/services, vendors, etc. with whom you have agreements. This Resource List will serve as a means of quick reference for getting needed services and supplies. Be sure to get 24-hour contact information.
2. Also in Section X of the Planner, list names, addresses and contact information for any other important resources.

## **G. Unique Needs**

List any special needs which may be unique to your operations such as special equipment, unique skills needed to recover, etc. Include these needs in Section XI of the Planner. Before you are finished with the planning process, take these needs and integrate them into the appropriate parts of the Plan.

### **III. Where to go from here**

#### **A. University-wide Planning**

Since each Operating Unit of the University is unique, we cannot apply a blanket plan on the entire institution. So, the work of developing the plans must be done at the Unit level. However, you are not alone in this effort. Here are some other resources that can assist you:

1. For general questions about the nuts and bolts of planning, review of your planning documents, etc., contact the office of **Business Continuity Planning** at **(704) 687-2740**.
2. For questions regarding data protection, systems and automation, contact **ITS** at **(704) 687-3100**.
3. For questions regarding telecommunications (voice) contact **ITS (Telecommunications)** at **(704) 687-3100**
4. For information and assistance with determining physical safety issues (e.g., fire alarms, evacuation plans and procedures) contact **the Office of Environmental and Occupational Safety and Health** at **(704) 687- 4291**.
5. For information and assistance with identifying resources for off-campus work space contact **Facilities Management** at **(704) 687-2154**.

#### **B. Website**

The UNC Charlotte Business Continuity Planning web site can be viewed at <http://www.uncc.edu/bcp>.

#### **C. Reformat and Review**

When you have completed the steps in this workbook, the Planner will contain all of the information that you need for your plan. It is important that you now take this information, and review it to ensure that the document can be **used**.

1. This may mean that you will have to reformat the document. Also, we recommend that you fill in the flow charts in the Planner. The Business Continuity Planner must ensure that everything is kept up to date. Individual team members may only need the checklists that affect their jobs.
2. You may also want to prepare a copy without addresses, phone numbers and other sensitive information for public scrutiny.

## **D. Designate your Emergency Operations Center (EOC) (Colleges, Divisions).**

List the primary site and at least one secondary (alternate) location in Section I of the Planner.

1. An EOC is a central location where the members of your Recovery Team can meet to deal with the disaster.
2. An EOC is not necessarily the place you will provide your services during the recovery. It is a command center and only those people necessary to control of the recovery effort should go to the EOC.
3. The EOC should have:
  - a) Access to restrooms.
  - b) Several telephone lines.
  - c) Computer(s) with Internet access.
  - d) Room for all Recovery Team personnel to meet comfortably for an extended period of time.

## **E. Exercise the Plan**

1. Hold a meeting or meetings with all employees to familiarize them with the plan and their individual roles.
  - a) Introduce the plan and its concepts.
  - b) Refresh knowledge of the plan.
  - c) Applies to all staff.
2. Conduct a Formal Exercise (see below for exercise types)
  - The goals of an exercise are to:
    - (1) Reveal planning weaknesses.
    - (2) Reveal resource gaps.
    - (3) Improve coordination.
    - (4) Clarify individual roles/responsibilities.
    - (5) Improve performance during the “real thing”.

### 3. Exercise Types

**Note:** Following are all of the exercise types. We do not mean to imply that you should go through all four types of exercise each year. We do recommend that you start with a “table top” exercise and that you conduct one or more drills annually. Once every few years, try a functional and a full-scale exercise.

a) Drills

- (1) Often a series of telephone calls to ensure that everyone knows whom they should call.
- (2) Test a single function.
- (3) Requires actual response by everyone.
- (4) Can be done several times per year without inconveniencing staff.

b) Table Top (low pressure)

- (1) Practice problem solving as a group.
- (2) Familiarization with plans and people.
- (3) Policy makers can be involved.

c) Functional (high pressure)

- (1) Time sensitive /time driven.
- (2) Tailored to specific goals (evaluate one or two recovery functions)
- (3) Takes place in EOC only

d) Full scale (high pressure)

- (1) Adds a field component.
- (2) Stresses communications to EOC.
- (3) Requires actual mobilization of people and equipment.

4. Document the exercise

- a) Date and time
- b) Names of all attendees and observers
- c) Goals of the exercise
- d) Results of the exercise

Note: These are not “tests”. No one “fails”. Something usually does not go as planned and this results in a need to edit part or your entire plan. The idea is to uncover these problems before an emergency occurs.

5. The Office of Business Continuity Planning can give you more information about how to conduct an exercise. Contact office of Business Continuity Planning, Room 421, Reese Building at (704) 687-2740.

## **F. Final Review**

Have members of the Management Team (see Section IV of the Planner) review the plan with this workbook. The reviewer should go through the work book line by line and compare it to the Planner. Initial each and every bullet point and paragraph as you identify the completed component in the planner. This will ensure that all minimums have been met.

## **G. Compliance Memo**

1. Each year, prior to June 30, send the attached memo to the Office of Business Continuity Planning, 421 Reese, 9201 University City Blvd., Charlotte NC.
2. The memo should indicate the name of your Operating Unit, the names and telephone numbers of the Unit Manager and the Business Continuity Planning Coordinator, the location of the master copy of your Plan (for review if needed during regular business hours), verification that the plan has been exercised, reviewed and updated during the past fiscal year.
3. A sample memo is available, although any one-page format will do.
4. **DO NOT send** a copy of the plan.

**THE UNIVERSITY OF NORTH CAROLINA AT CHARLOTTE**

**Business Continuity Planning Workbook**

# **Appendix**

## **Critical Business Processes of the University**

