IT Disaster Recovery Plan Template

CONTENTS:

Section 1 -- Scope and Size of Disaster Recovery Plan

A. Over-arching considerations

- Campus issues and checks:
  - Records management requirements by individual state
  - Requirement for business continuity plan (Definition: Business continuity plan is a customer's plan to delivery service "manually" while IT disaster recovery restores electronic service.)
  - HIPAA requires a disaster recovery plan
  - University is a "business" and there is a big loss to the student when business is out of order.
  - Do we need a business continuity plan for the students?
  - Need to be **practical** and **usable,** not just theoretical
  - Need to be understandable
  - Can't spend a lot of money

B. Determine Scope and Size

- Agree upon level of scope
- Can a "non-IT shop" person come in and understand the plan?
- Is the plan practical?
- Do we outsource the plan?
- Need to share examples
- Need to consider in overarching **Campus crisis plan**
  - Within this, need to include **master data center recovery plan**
    - Within this, need to include respective customer and individual service plans, e.g., PeopleSoft services, Mainframe services, enterprise storage services, individual customers' computers, etc.

Section 2 -- Definitions of Disaster

A. What are (and what are *not*) the criteria to determine a disaster?

- Physical, data, hardware
- How do we know if a disaster has been detected?

B. Examples of a disaster
    - Outage by hours
    - Outage by hours greater than certain level requiring contact of disaster team to declare disaster (for ex., notify campus crisis team)
    - When day-to-day plans no longer work (i.e., day-to-day work drill is gone, or when there is a build-up, escalation procedures are exhausted, and operation no longer meets common baseline planning
    - When there are threats that scope up to become a disaster (i.e., Sept. 11, campus unrest, etc.)
    - When we lose a data center or building that houses the data center
    - When we lose complete staff (labor resources) of data center
    - When we lose a core business service (i.e., email)
    - When we require Risk Mgmt and Insurance to declare a disaster in order to get vendor action in recovery
    - Need to share other examples of disaster in order to clarify for your own institution
    - Need to develop own definitions of disaster that are practical as opposed to industry definitions.

Section 3 -- Framework Design: Hardware and Software

A. Who is the vendor?
    - Proprietary (Sun Solaris, Linux, windows, AIX)
    - Homegrown (you are the vendor)
    - Mainframes
    - Needs Service Level Agreements (SLA) with vendors to replace the equipment if disaster strikes

B. Hardware configured environments (i.e., production, test, crash and burn, etc.)

C. What is your hardware asset inventory? (Let's share the data elements we are keeping about your assets.)
    - i.e., "Assets Center" by Peregrine; "LDR Plus" by Vendor?; Oracle database/homegrown systems (i.e., SOAPI)
    - Damage assessment by Risk management and insurance
    - Photos of equipment
    - Naming conventions of the hardware

D. Change information system (how do you make changes to your hardware environment?)

E. Tracking system for problems with hardware, applications, and network

F. Categories of operating system software

G. Proprietary factors of software

H. Redundancy of data

I. Backing up the software, data and OS

J. Storage
    - Single copy
    - Redundant copy
    - Security of data, software and applications

- How do you test for this item of disaster?

K. Enterprise systems
L. Client server services

Section 4 -- Framework Design: Environmental

A. One data center or Multiple data center sites
B. What are your campus building plans? Tag a 2nd data center into new building plans;
C. Hot site (exact duplicate of data center site)
D. Warm site (physical site and certain aspects ready, but need servers)
E. Run at another site but at a lower capacity (not hot, warm, but operable)
F. Cold site (we have a room and everything has to be planned)
G. Physical security system for site
    - Re-entry after disaster
    - Protection and Safety of disaster site
    - Silent panic button
    - Who issues building "all clear?"
    - Check out 911 service in relation to disasters
    - Flood plain of the site
    - Water detection at the site
    - HVAC at the site
    - Cooling glycol inventory
    - "run wet" (use of chilled water to control room temperature)
    - Fire suppression (Halon)
    - Alternate power sources
    - Diesel generators
    - Check diesel levels
    - Uninterruptable power source (UPS)
    - Batteries
    - Do you have UPS on individual computer systems? (Check out electrical certification of this with local campus electrical shop and then figure out how to test.) (NOTE: This is NOT a good idea.)

Section 5 -- Framework Design: Customers

A. Business continuity plan (customers should be asked how they will operate their business while they are down)
B. Business impact analysis (rate the impact of your services to determine how and when to bring your service back up
C. Webification of customers' applications, global use versus local client use on campus.
D. Priority processing—campus customer calendar
E. Ranking Business Processes (i.e., Core, T1, T2, T3, etc.)
    - PeopleSoft
        - Student systems
        - Financial systems
    - Payroll
    - Multi-campus based courses/distance education class

- "Research" customers (as a Core process)

F. Service Level agreements with customers
   - Need customer organization charts for DR
   - Determine amount of money for instantaneous disaster recovery or delayed disaster recovery

Section 6 -- Framework Design: Labor Resources

A. Staff availability
   - Depends on the disaster; have staff been wiped out by the disaster? (i.e., weather disaster, physical disaster, etc.)

B. Staff dependability/reliability
   - Union agreements/labor contracts
   - Who does what in a disaster?
   - Are staff excellent in day-to-day but horrible under pressure?
   - "Burnout" of staff during disaster
   - Are there any SLA (support level agreement) with peer agencies (state or other IT campus agencies)

C. Counseling services availability
D. IT Management tier (see cultural, political, financial)
E. Top campus mgmt (see cultural, political, financial)
F. Mass campus retirement—how to replace expertise?
   - How do we teach others before they retire?

G. Accounting for labor resources with reorganization processes
H. Vendor consulting services—do we use vendors as a resource for DR staff (could be for one person or a whole team)?
I. Escalation team (separate from DR team or day2day—decide when to escalate)
J. Disaster recovery team
K. Restoration team
L. Day-to-day Operation team

Section 7 -- Framework Design: Networking

A. Topology map of the network
   - Inter-company collaboration
   - Incorporate webification of services over the network
   - Redundancy
   - Each campus' expansion within its own state (IN's I-Light project and UW-Mad with WiscNet)

B. Other characteristics of networking
   - Duel network feeds to site
   - Dark Fiber requires multiple paths
   - Underground or overhead
   - Satellite feeds?
   - How do you replace the "Support equipment" to monitor and maintain topology?

Section 8 -- Framework Design: Cultural, Political, Financial

A. **KEY ITEM:** Buy-in and support by top mgmt on campus from beginning (i.e., chancellor or provost)
B. Money/budget/financial for DR—where from??
   - Who has the purse?
   - Is it funded by infrastructure?
   - Is it funded by each individual customer service?
   - Is it part of technologist's fee? ("tack on")
C. Campus crisis planning
   - IT disaster recovery plan and IT disaster services recovery plan should be an item on campus crisis plan
D. Terrorists (Sept. 11, disgruntled grad students?)
E. Staff acceptance
F. Customer acceptance
G. Auditor's acceptance
   - Main doorway for most disaster recovery planning
H. Campus records bldg (where do they reside)
I. Relation of IT DR to physical plant and other campus infrastructures

Section 9 -- Administrative Processes

A. IT Organization Chart for DR (and customers' Org chart)
B. Initial response notification
   - Calling tree
   - No phone service available? "Radio communications"; batteries? Which top offices will have radio communications available—need to document
C. Communication to external media (via IT media person or Campus Crisis media person)
D. Who signs off and authorizes which team?
E. Each campus needs to define its own administrative processes and protocol.

Section 10 -- Logistical Processes

A. Temporary Workspace/physical
B. Setup a temporary command center
C. Provide telephone lines to command center
D. Time elements of the plan
E. When do "Disaster Recovery Operations" (for a customer or service) end and day-to-day operations begin?
F. Each campus needs to define logistical processes

Section 11 -- Testing Processes

A. Each campus needs to define the testing process
   - Define testing process for each aspect of "how to test" the component pieces
     - IT processes
     - Administrative processes
     - Logistical processes
B. Examples of testing include:
   - Structured walk-through (possibly including other IT staff)

- Once/year annual audit (ex. Payroll checks)
- Include customers' business continuity plan
- Matrix of options; what is "standard" or "Benchmark" for testing?
- Easier to test "everything" than to test the parts
- What about loss of labor (for ex., death, injury, incapacity) and how to test this (See Section 6—Labor Resources)

Section 12 -- Training of Staff on Plan

A. What is the Objective of training?
   - Heighten awareness
   - So a new person can get through DR education
   - Ensure that it is "practically" understood.
     - Do you "read the book" or do you "show how"

B. Who is cross-trained for DR?

C. Where is documentation for DR located? (i.e., DR team members' homes, trunks of their cars, etc.)

D. Could IT Disaster Recovery group assist each other with training?
   - Do individual institutions have an IT training department that could assist?
   - Can our individual institutions' IT data center staff train each other?

Section 13 -- Maintenance of Plan

A. Documentation repository

B. Plan must be maintained annually, BUT parts of the plan need to be updated more frequently (for ex., phone lists)
   - Plan should be in a dynamic database that can be updated automatically

C. "Who does what" for DR plan maintenance?
   - Who updates what section?
   - Prints copies of the plan?
   - Who files the plan?
   - Kept with which members at home or in trunk of car?
   - Kept on wallet card? (DRP team instructions)
   - Who keeps log for audit of the maintenance?

D. Changes to the asset inventory should automatically update the disaster recovery plan

E. Problems with testing the plan should cause an update of plan

F. Annual agreement by top campus management to keep plan at level of funding, etc.

G. Return to Day-to-Day Operations
   - Have maintenance agreements in place
   - Have customer service level agreements in place (sign-offs)

H. "Lite" version of plan—also see Section 1—Scope and Size
   - Provides some preparedness for DR;
   - Drives items for more detail of DR
   - Could be an interim plan; if "this", then we do "that"
   - Could mitigate or lessen disaster
     - Who responds
     - How does it get resolved

    - How can we prevent it
- A road map to assist with the check-off process to make sure everything has been recovered