Print

Disaster Plan Checklist

This file is used in conjunction with the **Disaster Prevention - a generic overview** document. It is beneficial to read the related document before using this checklist.

Define the core business by levels of criticality.

- √ Level 1: Product(s) or service(s) that generate income
- √ Level 2: Service(s) that directly support Level 1, such as:
    - √ Receiving/Shipping
    - √ AR/AP
- √ Level 3: Other services

Determine what can/should/must be covered by insurance (building, major capitol equipment, etc.)

Determine what can/should be covered by self-insurance (disposable products)

Define acceptable "out-of-service" times for Level 1, Level 2, and Level 3 operations

Define requirements to maintain Level 1 operation

- √ Personnel
- √ Facilities
- √ Power
- √ Communication (commercial, private networks; WANs, LANs)
- √ Computer hardware and software (include Y2K concerns)

Define requirements to maintain Level 2 operations

    - √ Same as Level 1.

Define requirements to maintain Level 3 operations

- √ Same as Level 1.

Identify backup options for Level 1 and Level 2 operations

- √ Same company/same site (redundant equipment, spares parts, software)
- √ Same company/different site (excess capacity or additional equipment required)
- √ Related company/different site (excess capacity or additional equipment required)
- √ Commercial backup provider (equipment commonality and capacity concerns)

Identify backup currency for all operation Levels

- √ No interruption (mirror site hot backup; continual connection between like equipment)

- √ Minimal interruption (less than 30 minutes - update data every 30 minutes)
- √ Continue extending time as required.

Identify off-site location for backup/archives of end-of-(shift/day) backup files

Define potential disaster causes - a partial list includes:

- √ Communications failure (Internet, intranet [LAN, WAN], private telecomm net)
- √ Communications failure (public, private telco network)
- √ Earthquake
- √ Electrical supply failure
- √ Fire
- √ Flood
- √ Humidity (low/high)
- √ Hurricane/Typhoon
- √ Mud slide
- √ Sabotage (competitor, (ex)-employee, terrorist, vandal)
- √ Temperature (low/high)
- √ Tornado

Define segments ("links in the chain") for communications failures (servers, routers, hubs; business line, CO, etc.)

Define preventive measures for, and means to mitigate damage from, each potential disaster cause

Inventory and test detection/protection equipment

Identify personnel in each department to represent the department on a Disaster Recovery Team (DRT).

Identify two people to head the DRT; one a DRT Leader and one as DRT Deputy Leader

Narrowly define roles for DRT Leader, DRT Deputy Leader, and DRT members.

Define action-to-take for each disaster type; include all steps from "Call 911" to "Evacuate and assemble at ..."

Define decision making process to declare a disaster

Define steps to move Level 1 operation to backup site(s)

- √ Notify backup site to (prepare to) take over
- √ Notify local personnel of temporary duties

Define steps to move Level 2 operations to backup site(s)

Same as Level 1

Define steps to maintain Level 3 operations to "best available status"

Notify local personnel of temporary duties

Define steps to return operations to local operation.

Define method to test disaster plan.

Test plan.

Revise plan.

Set time to annually test/update disaster plan.

For additional information and disaster prevention planning contact

John Glenn
DMR Consulting Group Inc.
Voice: 800.338.7326 * Fax: 813.888.5334
Email: johnglenn1943@yahoo.com