Disaster Recovery Plan Test Template

The testing of a Disaster Recovery Plan will primarily be based on your actual plan. This plan could be “on the back of an envelope” or as comprehensive as the attached Disaster Recovery Template.

The plan should be set up in a way that a “relevant” new member of staff should be able to project manage a full Disaster Recovery Plan.

Depending on your requirements the testing could be based on the IT system only or could be tested as part of a more comprehensive Business Continuity Plan similar to the attached.

Without seeing your Recovery Plan it is difficult to map out a testing schedule. Realistically, the plan should be incorporating some of the following points. However, if not included in your plan then you might consider these points when reviewing the results of the test…..which might improve the quality of the revised Disaster Recovery Plan

1. Why are we testing the Disaster Recovery Plan?
2. What are we expecting from the testing?
3. What is a measure of success – Success may be a full remote recovery…but could also be non-recovery but identifying the gaps/tripping points in the system which will improve for the next time
4. Does the plan work
5. Is the plan up to date
6. Who has access to the Plan?
7. Who is to run the Disaster Plan? What happens if key person(s) is missing
8. Who is on the Phone List Matrix (effectively the next of kin list)? Again, is the plan up to date?
9. A side benefit of testing is training for Project Participants
10. Are all IT Assets comprehensively documented (hardware & software).
11. Identify the mission critical hardware as well as mission critical data/software.
12. Another side benefit will be to raise profile of importance/security/integrity of data
13. Consider give a copy of Disaster Plan and test results to Auditors/Banks
14. Who has authorised this work – needs approval by CEO/CIO/Managers eg. need total company buy in.
15. Checking data is the Min. objective. The test should cover far more.
16. Draw up clear Test Plan
17. Draw up clear Objectives
18. Set out Goals, eg. our goal is to set up a new server in a remote location with mission critical information within 8 hours.
19. Big impact from this goal. Who defines Critical? Does the whole company agree with this? Is this practical. Also, worth agreeing what is Non critical information and set a time frame for restoration of this.
20. Probably load Recovered data to a virtual server in our remote Facility.
21. To assume Broadband line will be running is a dangerous assumption!!!
22. Disasters are not more common…but our data is more vulnerable.

23. What technologies are included in the Disaster Recovery Plan and Test? Server / Phones Systems / Desktops / Switches / Laptops – location of same.
24. Determine what resources will be needed to conduct the test.
25. Define and document all the steps to be taken in the course of the test; this is the script for the test.
26. Then review the test plan and script with all IT resources needed for the test.
27. Obviously, AVOID creating a disaster via the test.
28. NO Cheating!! No Shortcuts. No use of secret knowledge/passwords. If not documented then cannot be used.
29. Run the plan and document any and all required changes or extra info.
30. Once the test is completed and systems have been returned to normal, have a post-test review as soon as possible after the test to determine what worked, what didn't work, and lessons learned.
31. Update DR processes and procedures as soon as possible with information from the test.
32. Finally, schedule the next test -- frequent testing is critical.