

Disaster Recovery Checklist

DISASTER RECOVERY PLANNING	Yes	No
The Plan - Technology		
Do you have a written Disaster Recovery Plan?		
Is the Plan current?		
Have you tested the Plan?		
Have legal or regulatory compliance requirements been addressed in the Plan?		
Are all of your critical data and applications (including email) part of the Plan?		
Is there a clear Recovery Time Objective for each business requirement?		
Is that Recovery Time Objective tiered based on criticality to the business?		
Do you have a designated recovery site for data?		
Are hardware, software, facilities, and service vendors part of the Plan?		
Do the vendors know your expectation of them in the event of a Disaster?		
Is critical data backed up on a frequent and regular basis?		
Are backups located off site?		
Are backups tested?		
Are you located in a mandatory evacuation zone?		
The Plan - People		
Does the Plan include employees (with current contact info) critical to recovery?		
Do those employees know their role in the Plan?		
Can the recovery be executed by individuals who are not "experts"?		
Do you have a designated recovery site for people?		
Will your staff relocate?		
Has your staff participated in an actual test of your Disaster Recovery plan?		
Does your staff have access to documentation online and offline?		
Do you have an alternative if your staff is not available during an actual disaster?		
Do you require contractors or business partners to be available?		
Do those contractors/partners know about your plan and expectations?		
Do you have an alternative if your contractors/partners are not available?		
SECURING YOUR PRIMARY INFRASTRUCTURE/PLATFORM	Yes	No
Data Center		
Is your platform for critical data and applications located in a secure Data Center ("DC")?		
Is access to the DC secured with badge, PIN, biometric?		
Do you have access to a second DC networked to/with the primary DC (hot or cold)?		
Does your DC monitor and ensure proper temperature and humidity?		
Does your DC have adequate fire suppression?		
Is your hardware adequately secured and monitored inside the DC (rack or cage)?		
Does your DC provide fully conditioned power to all Hardware?		
Does your DC provide redundant power with a UPS and generator?		
Does your DC have a power plan and scheduled maintenance?		
Does your DC test on a regular basis?		
Network		
Does your network have multiple fiber connections (sonet rings) with dual entry points?		
Do you have multiple carrier class ISPs to the Internet?		
Is your network fail over integrated into the Network topography?		
Do you perform BGP Routing to mitigate fail over?		
Data Protection and Support		
Is your data automatically backed up daily?		
Do you secure backup data off-site?		
Do you have a comprehensive security strategy with policies and procedures in place?		
Does your data have virus protection?		
Do you perform intrusion detection?		
Is your firewall managed and monitored?		
Do you employ or have access to live engineers 24x7x365?		



Disaster Recovery Checklist

Real Lessons from Real Disasters

"Nearly half the companies that lose their data through disaster, never re-open, and 90% are out of business within two years." (source - University of Texas Centre for Research on Information Systems)

Lesson #1: Staff may not relocate or be available

- Priorities are still at home
- Need to cross train staff
- Develop clear documentation
- Verify your strategy

Lesson #2: The "declare" decision is difficult -- Extend contingencies

- Ensure adequate supplies (i.e., paper, forms, etc...)
- Well thought out method of operation

Lesson #3: Situation not anticipated; simply inadequate planning

- Expect the un-expected

Lesson #4: Larger call or transaction volumes than planned for

- Concern & Curiosity
- Plan for size
- Typical volume goes up 3X during a disaster

Lesson #5: Something will go wrong

- Alternatives for resources, strategy, solutions
- Practice, practice, practice
- Initiative and ingenuity

The above questions should be considered when implementing the best solution to avoid business interruption caused by disaster (natural or otherwise) and to recover as quickly and efficiently as possible should a disaster occur. To find out how Peak 10 can help, please visit us at www.peak10.com or call one of the professionals below.

Jacksonville Facility, Allen Skipper -- General Manager
904.279.1777 or jacksonville@peak10.com

Tampa Facility, Debra Curtiss -- General Manager
813.675.1010 or tampa@peak10.com

Raleigh Facility, Greg Rollet -- General Manager
919.379.1010 or raleigh@peak10.com

Charlotte Facility, Pat O'Brien -- General Manager
704.264.1010 or charlotte@peak10.com

