

Business Continuity/Disaster Recovery Checklist

“Failing to prepare is preparing to fail,” according to John Wooden the most winning basketball coach in the history of the NCAA and he could just as well have been talking about Business Continuity and Disaster Recovery as winning basketball games. Comprehensive, detailed planning is the foundation upon which every successful Business Continuity and Disaster Recovery strategy is built.

Until recently, the primary focus of Business Continuity/Disaster Recovery plans were the safety and security of computer hardware and software applications running on an IT infrastructure. Increasingly, business and non-business institutions alike are recognizing any failure, much less a prolonged failure, of their primary IT operation can profoundly affect their ability to function and in the extreme threaten their very survival. As a result, business and non-business institutions alike are broadening the scope of planning which underpin their Business Continuity and Disaster Recovery strategies to involve not only IT personnel but the entire senior management staff. Core issues such as: which applications are critical to assuring the continued operation of the organization; assessing and quantifying the impact of different levels and lengths of potential outages; identifying critical operating and administrative personnel required to keep an organization functioning and defining what minimum levels of information they need to function during a crisis; and what IT staff is required to operate a disaster recovery operation should an outage occur are being used to define the requirements of an organization’s Business Continuity and Disaster Recovery strategy.

Once an organization has defined the operating requirements of its Business Continuity and Disaster Recovery strategy, the IT organization will be in a position to evaluate offsite disaster recovery options including data center facilities, housing and office space for critical IT operating personnel, and communications areas. Having assisted well over 100 companies in defining and/or refining their offsite disaster recovery plans, Herakles has developed the following checklist of critical factors which are key to choosing a disaster recovery data center and offsite infrastructure which best meets the overall business continuity requirements of an organization.

Data Center Critical Criteria

General

- Building, land, and infrastructure is owned, not leased
If leased. termination notice, cancellation provisions,
 rent escalations
- Dedicated power source (substation)
- Single user power substations
- Proximity of major and secondary sub stations
- On-site labs
- On-site Receiving area
- Short and long term physical storage available
- Accessibility to the data center and work recovery area
- Very low risk from natural threats (earthquakes, hurricanes, tornadoes)
- Meets or exceeds seismic requirements for the region
- Availability of Enterprise Zone Tax Credits
- Facility fully build-out without major expansions planned
- Comprehensive operations manual



Mission-Critical Emergency Power Systems

- Multiple emergency generators
- Back-up electrical switchgear
- State-of-the-art paralleling hardware
- Multiple battery line ups
- Multiple UPS systems
- Automatic fail over to redundant systems
- Continuous power feeds through the battery lineups
- Electrical systems fully integrated with Building Management System

On-Site Fuel Supply

- Sufficient fuel for prolonged outages
- Multiple fuel supply contracts
- Priority of fuel delivery in emergency situations
- Fuel regularly sampled for stability

Minimum of N+1 Power Feeds up to the Client's Equipment

- Power redundancy directly to customers' equipment
- Automatic transfer switches in multiple critical lines
- Redundant Power Distribution Units (PDUs)
- A/B circuit availability

Minimum of N + 1 Redundant Cooling

- Multiple cooling plants
- Mechanical systems fully integrated with Building Management System
- Leak detection throughout raised floor
- Critical infrastructure availability (99.999%)

Physical and Electronic Security

- On-site professional security personnel on site 24/7/365
- Card readers, PIN code keypads and biometric readers
- Monitoring systems tracks and records access throughout the facility
- Pre-approved client lists with programmable multilevel access zones
- Event driven digital closed circuit TV cameras with digital archive
- High resolution Zoom cameras
- 360 degree perimeter and roof surveillance
- Smoke and thermal detectors integrated with internal and external monitoring systems
- State-of-the-art electronic security systems

Fire Detection/Suppression

- Intelligent smoke and thermal (heat) detectors integrated with internal and external monitoring systems
- System control panel to pinpoint fire location
- VESDA smoke detection system throughout colocation floor
- Thermal detectors - combination of fixed temperature and rate of rise detection devices
- Double interlock pre-action dry pipe system
- High temperature fusible sensors on fire sprinkler heads integrated with monitoring system
- Fail-safe alarm system to prevent false discharge

Network Solutions

- Technical staff on-site 24x7
- Ability to communicate with data center staff via multiple paths
- Network data security
- Ongoing network and system monitoring
- Multiple Internet and telecommunication providers
- Affordable fiber solutions
- On demand burstable Internet bandwidth
- Diverse entry of fiber through multiple points
- Multiple fiber vaults
- Physical access to equipment 24/7
- State-of-the-art infrastructure management systems
- Comprehensive, fully funded, preventative maintenance and testing of all critical systems
- On-site and off-site data storage and backup systems

Work Recovery Area

- Furnished office and work area space available on a dedicated and/or subscription basis
- Flexible time frames without forced move out dates
- UPS systems/backup power
- Connectivity to data networks
- Internet access to clients' hardware from work recovery area
- Dedicated telephone systems
- On-site security
- Availability of computer equipment
- Break areas, conference rooms and restroom facilities
- Close proximity to lodging accommodations
- Close proximity to *major freeways and a metropolitan airport*

Staff Qualifications

- Stability of technical and management staff (turnover)
- Written and monitored customer service policies
- Trained and certified technical personnel
- Personnel cross-trained
- Key personnel in close proximity to the data center

Even though this list was created to evaluate the qualifications of a data center to meet the specific needs of disaster recovery it can also be used to assess your primary site. When selecting a data center it is important that the facility meet at least 90% of the above listed criteria. If not, review your requirements or continue to search for a data center which meets or exceeds the criteria listed.