



# Disaster Preparedness Checklist for Business Owners



## + Planning for Impact

- Identify a coordinator/team with defined roles for preparedness & response planning
- Determine which processes/services are mission-critical to the survivability of the business
- Determine acceptable levels of service during the recovery period; what processes need to be maintained or restored first to keep the business running smoothly
- Identify essential employees & critical inputs (ie. logistics, vendors) required to maintain business operations during a disaster event
- Conduct a technology asset inventory to determine & document the mission-critical technology components, their location, how they're configured, & who is responsible for them
- Once key components are identified, what measures need be taken to protect & recover them?
- Understand any regulations governing your business. If your network went down would you be able to maintain compliance (HIPAA, Privacy, Sarbanes Oxley, etc.)
- Understand obligations to customers and partners from a service standpoint to avoid breaching any contracts and communicate service remedies when appropriate
- Set a budget: Quantify potential costs of downtime and total failure to allocate appropriate funds

## + Assessing your Data & Technology Needs

- Status of your existing disaster recovery plan: Is there one? Is it maintained? Is it tested?
- Determine the vulnerability of your technology infrastructure to natural disasters (hurricanes, fires, etc.) Set clear recovery time objectives for each of your business/technology areas
- Determine the need for off-site data storage and backup
- Develop a technology plan that includes hardware, software, facilities and service vendors
- Secure clear understanding and commitment from vendors on your plan
- Need a backup vendor? If someone else manages your network, are they ready for a disaster?
- Perform security risk assessments for specific threats where possible. Examples of data security: Virus protection, intrusion detection, hacker prevention, system crashes, etc.
- Determine effectiveness of your data backup/recovery policies and procedures. Are they fully documented and is a staff member responsible for maintaining and updating?
- Perform a data recovery test. SERIOUSLY. You don't want holes showing up during a disaster
- Prepare an incident response plan for mitigating a security breach. No one wants to deal with a data breach but you want to be ready if it does. Plan should be audited & revised annually as security threats will change over time

## + Communicating your Plan to Employees & Partners

- Who needs to be contacted with critical information? Build a distribution list & maintain for accuracy
- Develop a contact plan to reach employees: cell numbers, alternate contacts, home address, etc.
- Ensure employees know where to receive update/info about returning to work, working remote, etc.
- Ensure mission-critical employees know their role and have remote access (VPN for security)
- Determine if you need a dedicated recovery site to maintain business. Plan out set up if needed
- If you require support from vendor partners, ensure they also have a documented plan that complements your needs and review annually to stay current