**HURRICANE PREPAREDNESS**

**CHECKLIST**

|  |  |
| --- | --- |
| **IT INFRASTRUCTURE** | **DOCUMENTED?** |
| Document all servers   * Name * Location * Function * Software installed with versions * Network information |  |
| Document all internal wired networks   * Name * Network address * Purpose * Security settings |  |
| Document all internal wireless networks   * Name * Network address * Purpose * Security settings |  |
| Document all guest networks   * Name * Network address * Purpose * Security settings |  |
| Document Internet connections   * Service provider * Service provider account number * Service provider contact information * Connection type – fiber, coax cable, wireless, etc * Network addresses * Connection speed |  |
| Document workstations   * Name * Manufacturer * Model * Serial number * Manufacture date / age * Location * Purpose * Primary user |  |
| Document portable computers   * Name * Manufacturer * Model * Serial number * Manufacture date / age * Location * Purpose * Primary user |  |
| Document mobile devices – Phones, tablets   * Name * Manufacturer * Model * Serial number * Manufacture date / age * Location * Purpose * Primary user |  |
| Document printers, scanners, copiers, fax machines   * Name * Manufacturer * Model * Location * Network address * Purpose |  |
| Document IOT devices   * Include facilities devices like thermostats and security cameras * Include audio-visual devices like TVs and smart speakers * Name * Manufacturer * Model * Location * Network connected to * Purpose |  |
| Document all software   * Name * Publisher * Version * License * Where installed |  |
| Document cloud services   * Name * Purpose * Administrative credentials * Data stored |  |
| Determine what hardware, software, and data is critical to keep online during a hurricane and what can be taken offline temporarily during the event. |  |

|  |  |
| --- | --- |
| **DISASTER PLANNING** | **COMPLETE?** |
| Review backup systems   * Identify all data locations * Review backup method for each set of data * Review backup schedule for each set of data * Review recent backup logs to check backup is working |  |
| Verify offsite backup locations   * Verify all backups are copied to a secondary location or the cloud to eliminate a single failure point * Verify offsite backups are working * Verify access credentials for offsite locations |  |
| Ensure backups run on a schedule to match data sensitivity   * Determine what data is more static and needs less frequent backup * Determine what data is more dynamic and requires more frequent backup |  |
| Establish a timeline for IT recovery   * How long is acceptable for your IT systems to be down? * This is called RTO or recovery time objective * Plan accordingly – if you require a low RTO (fast recovery) you need spare equipment on hand or a DR site * As RTO goes lower (faster recovery) the complexity and expense required to meet that goes up. |  |
| Establish how much data loss you can accept   * How much data can you stand to lose from a failure? * This is called RPO or recovery point objective. * If you backup nightly, you have to be prepared to lose up to the full current day’s data. * If you backup hourly, you have to be prepared to lose up to the last hour of data. * As RPO goes shorter (less data loss) the complexity and expense required to meet that goes up. |  |
| Decide on your operational posture during a hurricane   * In the event of a tropical storm watch to your area, do you change operations? * A tropical storm warning? * A hurricane watch? * A hurricane warning? * A flood warning? * A high wind warning? * How do you respond to each situation? * When do you close your operations? * If you remain open, how do you address the situation? |  |
| Create contingency plans   * Who stays? * Who stops working? * Who continues work from another location? * Where is the other location? * Which functions or departments can be shutdown during an emergency and which cannot be? * Can personnel from functions that are shutdown help contribute to the functions that must continue? |  |
| Understand staff priorities   * Some staff may have to evacuate early if they are a caregiver to someone or due to other personal concerns * Can staff that may need to evacuate early help setup a remote operation outside the impacted area? * Who would be willing to volunteer to help respond to difficulties following a hurricane strike? |  |
| Establish procedure for alternate communications   * Decide how to communicate with employees and necessary personnel if normal communications are lost. * Plan for the possible loss of internet and/or cellular communications. * Ensure personnel know the alternate methods ahead of time * In the event of a loss of communications, where do you meet to reconnect? |  |
| Communicate to staff that remain on site what to do in the event of:   * Power loss * Lightning strike * Flooding * Internet outage * Equipment failure |  |
| Prepare staff that evacuate to another location   * Provide SECURE access to all work materials * Ensure internet capabilities and access * Supply hardware and software needed to work outside primary location |  |
| Create procedures to prepare ahead of the storm   * Move equipment off the floor in case of flooding * Unplug power to equipment in case of flooding or surge * Cover equipment with plastic sheeting in case of leaks |  |
| Create procedures to address physical damages that occur (flooding, power outages, etc.)   * Document how to respond to various problems including contact information for key staff, vendors, and contractors * Document how to move key equipment out of a facility if required |  |
| Consider insurance   * What coverage do you have? What is not covered? * How do you use your insurance if it is needed? Know the details ahead of time. * How much would a hurricane-related IT disaster cost you? |  |

|  |  |
| --- | --- |
| **DISASTER RECOVERY TESTING** | **TESTED?** |
| Test your entire disaster plan system at least once a year (preferably twice) |  |
| Test backup drives, cloud storage, etc. |  |
| Test equipment that would be taken off-site |  |
| Test internet and network connections in secondary work locations (secondary offices, homes, etc.) |  |
| Test emergency communications systems |  |
| Document what works well and what does not   * Improve where needed * Test again |  |

**Not ready? We are. Call us.**

**(813) 229-1700**

**(727) 280-5230**

**(352) 419-1166**