UNITRENDS

CHECKLIST

PREPARING FOR HURRICANE SEASON

Hurricanes are the costliest severe-weather events in recorded U.S. history. From 2018 to 2020, hurricanes accounted for 50 individual climate disasters, with damages in excess of $1 billion.[1]

The year 2021 was the second costliest year on record (2017 being the costliest), with insured losses amounting to more than $120 billion in hurricane-related damages.[2] Businesses today operate in a global, digital-first economy. It is vital that your organization is prepared to deal with the potential ramifications of hurricanes on your employees, operations and technology.

Not planning proactively for natural disasters like hurricanes can prove to be an expensive mistake that threatens the solvency of your business. A staggering 90% of SMBs close permanently if they fail to restore operations within five days of a disaster. The longer recovery takes, the more likely a business shuts its doors for good.[3]

In preparation for hurricane season, we've compiled a series of checklists to ensure your technology and data is secure and readily available for recovery in the event of a severe weather event or other disasters.

© 2022 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Establish (or review) your disaster recovery plan (DRP)

Your disaster recovery plan is critical during times of disruption. If you haven't **built your DR plan** yet, there's no better time to start than the present. If you have a DRP in place, revisit it. When was the last time your plan was updated or tested? **The checklist below outlines elements vital to building your DR plan:**

ITEM	DESCRIPTION	
Risk Assessment	The process to identify potential hazards and analyze what could happen should a disaster occur. Start by defining the disaster (natural, human-caused or technological) and the assets that are at risk. The safety of people should be the first consideration of any risk assessment.	☐
Business Impact Analysis (BIA)	The process to determine potential impacts that result from the interruption of time-sensitive services and critical business processes. When evaluating assets as part of your risk assessment, consider their vulnerabilities – weaknesses make an asset more susceptible to damage, contribute to the severity of an incident and can be used to direct your mitigation strategies.	☐
Recovery Objectives	Establish SLAs around acceptable Recovery Point Objective (RPO, how much data will we lose between backups) and Recovery Time Objective (RTO, how long will it take us to recover) for business assets. Recovery objectives may vary based on industry or differ between business units based on their priority to the organization.	☐
IT Asset Inventory	All IT resources – hardware systems, software, applications, networks and physical location of data centers – should be inventoried. Be sure to note different dependencies where they exist since that information will help speed up recovery efforts. Categorize systems by organizational priority.	☐
Roles & Responsibilities	Define the scope of roles and responsibilities of the various teams that fall under the DRP. These teams may include the Emergency Management Team (first response, damage assessment, BC/DR activation), Technology Support Team (establishes resources for emergency operations, recovery of key services, coordination with EMT and recovery of remaining infrastructure) and the BC/DR Team (ensures preparation and documentation, distribution of plans, ongoing assessment and evaluation, coordinating testing and plan walkthroughs).	☐
Emergency Response Actions	In the event of a building evacuation, define primary and secondary locations where employees should meet and outline a remote/WFH policy. Your DR plan should also address the use of emergency notification system from which employees receive updates (if applicable), as well as listing key contacts and how to reach them. Include manuals for automated notifications, mobile communications devices and social media.	☐
BC/DR Strategies	Define appropriate business recovery actions. These procedures should address recovery, restoration and resumption of mission-critical IT systems and networks following a disruption.	
Notification of BCP/DRP Activation	After the initial assessment and decision to activate the BC/DR plan, employees should be notified quickly, report to their supervisors and execute BC/DR activities as specified in the department-level BC/DR plans. Use a call tree, automated emergency notification system, smart phones, etc. Phoneline, SMS and/or email alerts should be used for employees to obtain updated information on the incident and report any new information that may be beneficial to manage the emergency.	☐
DR Plan Recovery Procedures	Define the appropriate business recovery actions. These procedures address recovery, restoration and resumption of mission-critical IT systems and networks following a disruption. The Technology Support Team will triage with the BCDR team to initiate the appropriate recovery and restoration actions to: • Address the specific incident • Ensure critical applications, platforms, virtualized infrastructure and data are accessible • Restore mission-critical network resources such as internet connectivity	☐
External Communications	The Public Relations Department (or any other approved department) should act as the principal point of contact for all media organizations, working within pre-established guidelines for media communications during and after an incident. Pre-configured press release forms and other such media documents will help facilitate communication. Only the approved department and personnel should be permitted direct contact with media; all other employees should be directed to the designated department for any requests for updates or other information sought by external parties.	☐

© 2022 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

The BC/DR Link

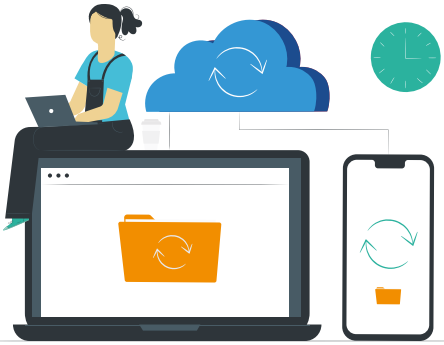
Relying solely on cobbled-together spreadsheets and word documents for your DRP complicates quick access to vital information during an emergency. The **BC/DR Link** by Unitrends is a free-to-use, ISO-certified BCDR plan template. Use the BC/DR Link to keep a centralized copy of your DRP accessible from any internet-connected device and print hard copies to store locally as required.

Safeguarding data technology before and during a hurricane event:

ITEM	DESCRIPTION	
Redundant Backup Copies	Performing backups and storing them locally helps recover from user error, hardware failures, accidental deletion and other events. Local backups should be used to create backup copies that can be stored in an alternate location. Redundancy protects local systems and primary backups by ensuring another copy exists that is not subject to an incident that affects the primary site.	☐
WAN-Accelerated Replication	Moving data over the WAN can be a cumbersome task, especially for larger data sets. Look for a solution that optimizes replication to efficiently move data from the source to the recovery target as quickly as possible in order to be ready for a disaster event. WAN optimization and acceleration technologies may include, but are not limited to, global deduplication, compression, encryption, source point querying, simple rate limits and bandwidth throttling.	☐
AES 256-bit Encryption	Encryption should be used to secure all data at-rest and in-flight. Backups should be encrypted to secure data and meet regulatory and corporate requirements to protect data from unauthorized access and theft. All data should remain encrypted until a request is made to restore the data.	☐
Cloud Replication	The accessibility of cloud infrastructure makes it a popular target for disaster recovery. Some providers tune their operations specifically to backup and DR use-cases. You should be able to failover any workload to a singular Disaster Recovery-as-a-Service (DRaaS) regardless of size, criticality or where it originated from. DRaaS providers serve as an extension of your team, orchestrating spin-up of technology resources during a hurricane event while you focus on the safety and security of your personnel.	☐
Recovery Testing	The only way to know you can recover after an emergency is to test regularly, especially when changes are made to your infrastructure. In addition to testing your DRP, backups should be tested regularly to verify their recoverability. New, intelligent tools are available for automated testing, ensuring all components are in place and recoverable. Look for a solution that integrates an automated recovery testing engine without the need for additional proxies or licensing.	☐
Protect Electronics	Secure windows and doors to buildings. Take additional steps to protect electronic systems from weather damage, including: • Moving electronic equipment to a safe room, away from windows and doors. • Storing electronics off the ground to protect from flooding. • Shutting down computers and unplugging machines and power protectors/surges. • Unplugging ethernet cables from computers and docking stations. • Unplugging printers, docks and other accessories. • Wrapping electronics in plastic or utilizing dry bags for protection against condensation in the short term.	☐

© 2022 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

Resilience and uptime with Unified BCDR



Unitrends Unified BCDR provides IT professionals with an integrated, cloud-empowered platform with the agility to protect traditional datacenter assets with **hybrid cloud appliances**. Pairing local appliances with Unitrends **Forever Cloud** enables secure, geo-redundant replication to secure a copy of your data outside the impact zone of a weather-related disaster. Supercharge your DR with **Disaster Recovery-as-a-Service**. As an extension of your team, Unitrends' cloud continuity experts spin-up and host mission-critical applications (or your entire datacenter) and help reroute user traffic to our cloud, enabling continuity when you can't get to the primary site.

Don't just take it from us! In the face of **hurricanes**, **tornados** and even **cyberattacks**, our customers have achieved innumerable wins against all forms of disaster. Want to learn more about how Unified BCDR can help your organization?

GET IN TOUCH TODAY!

ABOUT UNITRENDS

Unitrends makes efficient, reliable backup and recovery as effortless and hassle-free as possible. We combine deep expertise gained over thirty years of focusing on backup and recovery with next generation backup appliances and cloud purpose-built to make data protection simpler, more automated and more resilient than any other solution in the industry.

Learn more by visiting unitrends.com or follow us on LinkedIn and Twitter @Unitrends.

UNITRENDS
A Kaseya COMPANY

© 2022 UNITRENDS // ALL RIGHTS RESERVED // WWW.UNITRENDS.COM

PART #IN-9013-ENG-A