PHOENIXNAP'S DISASTER RECOVERY (DR) QUESTIONNAIRE

DISASTER RECOVERY 101

QUESTIONS	YES	NO	COMMENTS
Have you identified the critical operations and systems that require recovery in the event of a disaster?	○	○	
Do DR efforts have clear support and buy-in from the executive leadership?	○	○	
Does your DR plan have a clearly defined objective and scope?	○	○	
Did you prioritize goals (if you have multiple objectives)?	○	○	
Did you consult with key stakeholders during the objective-setting process?	○	○	
Must your DR efforts comply with any regulatory requirements?	○	○	
Have you allocated sufficient resources for DR planning and implementation?	○	○	

IT INVENTORY

QUESTIONS	YES	NO	COMMENTS
Have you identified all the hardware and software assets within your DR plan's scope?	○	○	
Is there a centralized document for tracking the IT asset inventory?	○	○	
Does the centralized document offer in-depth info about each asset (serial numbers, versions, configuration settings, dependencies, etc.)?	○	○	
Have you categorized IT assets based on criticality?	○	○	
Have you mapped all the data within the plan's scope?	○	○	
Did you assign a priority level to each IT asset and data set?	○	○	
Is there a defined process for documenting changes to hardware, software, or data sets?	○	○	

RISK ASSESSMENTS

QUESTIONS	YES	NO	COMMENTS
Have you identified risks and vulnerabilities for all relevant systems?	○	○	
Did you list all probable incidents and disruptions that could affect relevant systems?	○	○	
Have you evaluated the likelihood of each incident?	○	○	
Have you categorized IT assets based on criticality?	○	○	
Did you grade the potential impact of each identified event?	○	○	
Did you quantify the potential impact (where possible)?	○	○	
Were current risk assessments completed within the last 12 months?	○	○	
Have you performed a business impact analysis (BIA) for your systems?	○	○	
Were current BIAs completed within the last 12 months?	○	○	

RTOs AND RPOs

QUESTIONS	YES	NO	COMMENTS
Have you determined the maximum acceptable downtime for each critical system and operation?	○	○	
Have you calculated the maximum acceptable data loss in case of a disaster?	○	○	
Have you set the RTOs and RPOs for mission-critical systems and data sets?	○	○	
Did you consider dependencies between systems or processes when setting RTOs?	○	○	
Do RTOs and associated costs align with available resources?	○	○	
Do RPOs and associated costs align with available resources?	○	○	
Have you implemented measures to ensure systems are recoverable within the defined RTOs?	○	○	
Have you implemented measures to ensure data recoveries meet the defined RPOs?	○	○	
Did you communicate your RTOs and RPOs to relevant stakeholders within the organization?	○	○	

EMPLOYEE SAFETY

QUESTIONS	YES	NO	COMMENTS
Does the DR plan account for the safety of employees during incidents?	○	○	
Have you identified potential hazards and risks that could threaten employee safety during a disaster?	○	○	
Have you developed an emergency evacuation plan to ensure a safe exit from the premises during a disaster?	○	○	
Have you conducted drills to test the effectiveness of the emergency evacuation plan?	○	○	
Have you established designated post-evacuation assembly points for employees to gather after a disaster?	○	○	
Do RPOs and associated costs align with available resources?	○	○	
Have you implemented a system to account for all employees during evacuation?	○	○	
Does the workforce understand how to maintain business continuity safely following an incident (remote work arrangements, alternative work locations, temporary relocation options, etc.)?	○	○	
Have you installed appropriate safety equipment (fire extinguishers, emergency lighting, first aid kits, flashlights, etc.)?	○	○	
Have you established a communication plan to relay important safety info to the workforce before, during, and after an incident?	○	○	

PROACTIVE PREVENTION

QUESTIONS	YES	NO	COMMENTS
Does your DR plan include security measures that prevent cyber attacks and unauthorized IT access?	○	○	
Are there clear and documented procedures for reporting potential security breaches or safety concerns?	○	○	
Does your DR plan include physical security measures that prevent unauthorized entry or theft?	○	○	
Have you implemented proper fire and electrical safety measures?	○	○	
Do you have backup systems or redundant infrastructure to minimize the impact of hardware failures?	○	○	
Do you have a data backup strategy to protect against data loss or corruption?	○	○	
Do you perform regular inspections to identify and address potential equipment or infrastructure issues?	○	○	

DATA BACKUPS

QUESTIONS	YES	NO	COMMENTS
Do you regularly back up critical business data?	○	○	
Can current data backup strategies meet your expected RPOs?	○	○	
Do you use both on-site and off-site backup solutions?	○	○	
Do you encrypt backup data?	○	○	
Do you rely on periodic testing to verify the integrity of backups?	○	○	
Do backup copies reside in a secure and controlled environment?	○	○	
Do you use redundant systems to minimize the risk of backup failures?	○	○	
Do you have a documented process to restore data from backups during a disaster?	○	○	
Do you regularly review and update your backup strategy to adapt to changes in data lifecycles and business requirements?	○	○	

INCIDENT RESPONSE STRATEGY

QUESTIONS	YES	NO	COMMENTS
Did you base your incident response strategy on asset criticality and RTO requirements?	○	○	
Have you developed a documented incident response plan for most or all possible types of disasters?	○	○	
Does the DR plan have a clear response (invocation, resumption, and recovery) that progresses from disruption to resumption of normal business operations?	○	○	
Does the plan have an auditable process for tracking and recording the completion of tasks?	○	○	
Does the plan have clearly defined, documented, and approved KPIs?	○	○	
Does the plan have clearly defined invocation and escalation processes?	○	○	
Do you provide detailed failover and failback instructions?	○	○	
Have you identified and documented the roles and responsibilities of go-to personnel during an incident?	○	○	
Is there a process for collecting evidence related to the incident for potential investigations or legal purposes?	○	○	
Is there a post-recovery verification process?	○	○	
Do you conduct regular exercises to ensure employees are familiar with the incident response procedures?	○	○	
Is there a post-incident review process to evaluate the effectiveness of the response and identify areas for improvement?	○	○	

DISASTER RECOVERY SITES

QUESTIONS	YES	NO	COMMENTS
Do you have a secondary off-site location for disaster recovery purposes?	○	○	
Did you consider cold, warm, and hot secondary sites?	○	○	
Did you consider using the cloud to set up a recovery site?	○	○	
Is the secondary site geographically separate from your primary site?	○	○	
Is the secondary site equipped with the necessary infrastructure and resources to support critical business functions?	○	○	
Is there a mechanism to replicate or synchronize data between primary and secondary sites?	○	○	
Is the secondary site regularly tested to ensure its readiness to take over operations during a disaster?	○	○	
Do you have a defined process for activating the secondary site in the event of a disaster?	○	○	
Can the secondary site handle the anticipated workload and user demands during a disaster?	○	○	
Is the secondary site regularly reviewed and updated to reflect changes in your business requirements and technology infrastructure?	○	○	

TEAM BUILDING

QUESTIONS	YES	NO	COMMENTS
Have you identified key personnel responsible for leading and managing the disaster recovery process?	○	○	
Did you consult with team leads about what they require to meet the set RTOs?	○	○	
Have you defined the roles and responsibilities of each team member within the DR team?	○	○	
Have you provided training to team members to prepare them for their DR responsibilities?	○	○	
Have you identified backup members for critical roles in case of unavailability?	○	○	
Do you regularly review and update the composition, roles, and responsibilities of the DR team to reflect changes in your organization?	○	○	

COMMUNICATION STRATEGIES

QUESTIONS	YES	NO	COMMENTS
Do you have a communication plan to ensure effective coordination and info-sharing among the DR team members?	○	○	
Have you identified and documented the contact info for go-to personnel and stakeholders?	○	○	
Is contact info for all DR personnel (stakeholders, employees, response team members, etc.) up to date?	○	○	
Are there communication trees that outline the hierarchical communication order?	○	○	
Does the plan include a list of necessary service providers and suppliers?	○	○	
Does the DR plan include a list of emergency responders (e.g., police, fire, or EMT)?	○	○	
Have you established escalation procedures to ensure timely and appropriate decision-making?	○	○	
Are there alternative communication channels in case primary methods become unavailable during a disaster?	○	○	
Do you have a process for regularly testing and validating the reliability and functionality of communication channels?	○	○	
Is there a documented plan that outlines how teams share and communicate info during a disaster?	○	○	
Do you have priority communication protocols for critical messages?	○	○	
Does your DR plan require a section on dealing with the media and the public during and following a disaster?	○	○	

TESTING PROTOCOLS

QUESTIONS	YES	NO	COMMENTS
Do you regularly test your disaster recovery plan to validate its effectiveness?	○	○	
Do you set specific objectives and success criteria for each test?	○	○	
Do you document and analyze the results of each test to identify areas for improvement?	○	○	
Have you addressed any issues or deficiencies identified during testing?	○	○	
Do you conduct unannounced tests to assess the real-life DR readiness of your personnel and systems?	○	○	

KEEPING DISASTER RECOVERY UP TO DATE

QUESTIONS	YES	NO	COMMENTS
Do you audit DR plans at least once per year?	○	○	
Do you incorporate lessons learned from incidents into your response strategy?	○	○	
Do you keep your DR strategy up to date with the latest threats and industry best practices?	○	○	
Is DR planning a part of the corporate change management process?	○	○	
Do you review your DR plan every time you make a significant update to your IT?	○	○	
Is the DR plan a part of your broader IT strategy plan?	○	○	