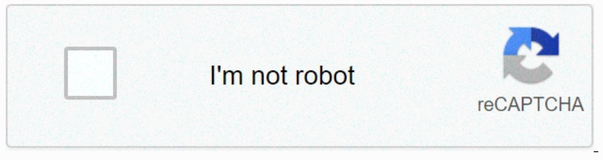

Continue

Network disaster recovery plan template

View a Cloud Based DR SolutionView a Cloud Based DR SolutionInformation Technology (IT) has redefined the global business lifecycle. Networking and communication have accelerated and made business operations more flexible. The Wide Area Network (WAN) and related technologies are the keys to efficient business operations in the competitive market. Companies adopt technologies and standards to keep their IT infrastructure solid and ensure business continuity. A company's continued operations are determined by its ability to manage potential natural or man-made disasters by creating an effective IT Disaster Recovery Plan (DRP) that can minimize network disruption and quickly restore operational normality. An IT Disaster Recovery Plan is a comprehensive documentation of well-planned actions to be taken before, during, and after a catastrophic event. To ensure business continuity and the availability of critical resources in the event of disasters, the plan should be documented and tested in advance. This will help to speed up the process when the actual disaster or emergency strikes. The key to IT or network disaster recovery is readiness. The DR Plan is the master tool of IT-based and other organizations to protect their IT infrastructure, determine organizational stability, and systematically prevent disaster recovery. The main objectives of IT/Network Disaster Recovery Planning include: Minimizing business interruptionsMinimizing Risk of DelayEnsuring a level of securityEnsuring reliable backup systemsSupport in restoring operations with speedBusiness vulnerabilities is constantly increasing, and each organization is forced to create appropriate disaster recovery plans and use advanced technologies to keep your network secure and stable. Network-dependent organizations believe it is an absolute necessity to create disaster recovery policies and procedures to respond to the different circumstances and problems. In any organization preparing for disaster recovery, the three main issues that need to be taken into account are prevention, anticipation, and mitigation. Prevention is the act of preventing disasters that can be prevented. The anticipation is to plan and develop appropriate measures to counter unavoidable disasters. Damage limitation consists in effectively managing the disasters and thus the negative impact.IT disaster recovery planning provides a thorough analysis of the existing network structure, applications, databases, organizational setup and related details. It is important to define in the document the key components of the company, the disaster recovery team with contact details, recovery time target, and communication methods at the time of the emergency, alternative setup for the organization, and the master list of all inventory, warehouses, customers/suppliers, forms, and policies. The following are the steps that should be taken in the event of IT disasters. Should. planning:Constitute a Disaster Recovery Team: The organization should form a DR team to help with all disaster recovery operations. The team should be made up of core members from all departments with representatives from top management. The team will also be responsible for monitoring the development and implementation of the DR plan. Risk assessment: A risk analysis and a business impact analysis should be carried out, including the scope of possible natural and man-made disasters. By conducting an analysis of the impacts and consequences in disaster scenarios, the security of important resources can be determined. Prioritize processes and operations: The organization's critical requirements for each department must be determined in terms of data, documentation, services, processes, operations, critical resources, and policies/procedures. They should all be sorted and sorted by priority as essential, important, and not essential. Data collection: The complete data about the organization must be collected and documented. It should include an inventory of forms, guidelines, equipment, communications; important telephone numbers, contact details and customer data; description of equipment, systems, applications and resources; On-site and offsite location; Details of the backup storage setup and retention schedules; and other materials and documentation. Create the Disaster Recovery Plan: The DR plan should be created in a standard format that allows for detailing procedures and including essential information. All important procedures should be fully outlined and explained in the plan. The plan should have step-by-step details of what to do if disaster strikes. It should also include procedures for maintaining and updating the plan, with periodic review by the disaster recovery team and the organization's top personnel. Testing the plan: The developed disaster recovery plan should be tested for efficiency. Testing provides a platform on which to analyze what changes are required and make appropriate adjustments to the plan. The plan can be tested with various types of tests, such as.B checklist tests, simulation tests, parallel tests, full break tests, and so on. Developing a good IT disaster recovery plan will enable organizations to minimize potential economic losses and disruptions in an emergency. It will help in an organized way of recovery, ensure that the organization's resources are secure, and pave the way for business continuity in the most imaginative way. Required this Disaster Recovery Plan (DR-Plan) is the Source of all information describing the ability of organization name to survive a disaster, including the processes that must be followed to perform the recovery. Edit this section to meet the needs of your organization and make all lists and other copies relevant to your organization. Definition: Disaster Optional A A can be caused by many events that cause the Organization Name IT department to be unable to perform some or all of its regular roles and responsibilities for a specific period of time. Organization Name defines disasters as follows: Edit this list to reflect your organization One or more important systems are not functional The building is not available for an extended period of time, but all systems are functional within it The building is available, but all systems are not functional The building and all systems are not functional The following events can cause a disaster, so this DR document must be enabled: Edit this list to reflect your organization. Hardware Error / Server Room Problem Power Failure Theft Intentional Attack Human Error Required The purpose of this DR Plan document is to inventory the entire IT infrastructure and capture all information relevant to the organization's ability to restore its IT after a disaster and document the steps the organization will follow in the event of an emergency. The top priority of Organization Name is to implement the steps described in this DR plan to bring all groups and departments of the organization back to normal as quickly as possible. These include: Edit this list to reflect your organization. First Name Last Name Title Contact Type Contact Information Employee F Employee L Title Work 555-555-5555 ext. 555 Mobile Alternate Email Work Mobile Alternate Email Work Mobile Email Last Name Last Name Title Contact Type Contact Address Property Manager / Landlord Account: Work Mobile Email Power Company Account: Work Mobile Email Security Company Account : Work Mobile Email Network Provider Account : Work Mobile Email Telecom Carrier Account : Work Mobile Email Managed Services / Help Desk Account •: Work Mobile Email Server Supplier Account : Work Mobile Email Workstation Supplier Account : Work Mobile Email Insurance Account : Work Mobile Email Off-Site Storage Account : Work Mobile Email Power Generator Account : Work Mobile Email Other Account : Work Mobile Email Required The DR plan takes into account all following technology areas: Edit this list, to your organization Network Infrastructure Servers Infrastructure Telephony System Data Storage and Backup Systems Data Output Devices End user Computer Organizational Software System Database Documentation : This DR plan does not take into account non-IT, personnel, personnel and real estate disasters. Required changes, changes, and updates to the DR plan recorded here. It is the responsibility of the Disaster Recovery Lead to ensure that all existing copies of the DR plan are up-to-date. When the DR plan is updated, the version number must be updated to indicate this. Add rows as needed when the DR plan is changed. Name of the person making change role of the person, the modified date of the change version number notes Bob Jones DR Lead 01/11/17 1.0 First version of DR Plan Bob Jones DR Lead 01/01/18 2.0 Revised, to replace new Evolve IP availability zones Lisa Smith CEO 04/03/18 2.1 Replacing Bob Jones as DR Lead Required In the event of an emergency, various teams are required to assist the IT department in their efforts to restore the organization name's employees to normal functionality. The various teams and their responsibilities are as follows: Edit this list to your organization Disaster Recovery Lead(s) Disaster Management Team Applications Team Teams Team The members of the Disaster Recovery team are responsible for performing all the tasks listed below. In some disaster situations, members of the Disaster Recovery Team are prompted to perform tasks that are not described in this section. The following teams vary depending on the size of your organization. Some teams/roles can be combined or split into more than one team. Required The Disaster Recovery Lead is responsible for all decisions related to disaster recovery efforts. The primary task of this person is to lead the disaster recovery process, and all other people involved in the disaster recovery process will report to that person in the event of an organization name disaster, regardless of their department and existing managers. Every effort is made to ensure that this person is separated from the other disaster management teams in order to keep their decisions unbiased. Therefore, the Disaster Recovery Lead is not a member of other disaster recovery groups in Organization Name. Edit this list to reflect your organization. Initiate the DR notification network. Be the one-stop shop for all DR teams and watch them. Organize and lead regular meetings of the DR team throughout the disaster. Present the status of the disaster and the decisions that need to be made to the management team. Organize, monitor, and manage all DR plan tests and create all DR plan updates. OPTIONAL The disaster management team that oversees the entire disaster recovery process and is the first team to take action in the event of a disaster. This team evaluates the disaster and determines the steps are around which the return to business as usual. In a small organization, these roles can be performed by the Disaster Recovery Lead. Edit this list to reflect your organization, set the DR plan in motion after the Disaster Recovery Lead has reported an emergency Determine the size and class of the emergency Determine which systems and processes are affected by the disaster. The disaster recovery process Ensure that all decisions made under the DR plan and the policies set by Organization Name prepare the secondary site for business recovery Ensure that the secondary site is fully functional and secure. Create a detailed report of all the steps that are performed in the disaster recovery process, notify the relevant parties when the disaster is over and normal business functionality is restored after the organization name is back up and running. this team will summarize all costs and provide the Disaster Recovery Lead with a report summarizing its activities during the emergency. The network team is responsible for assessing damage specific to a network infrastructure, as well as providing data and voice network connectivity, including WAN, LAN, and all telephony connections internally within the organization, as well as telephony and data connections to the outside world. You are primarily responsible for providing basic networking capabilities and can support other IT DR teams as needed. Edit this list to reflect your organization In the event of an emergency that does not require migration to/from Evolve IP availability zones, the team determines which network services will not work in the primary availability zones If multiple network services are affected, the team prioritizes restoring services in the manner and order that has the least business impact. When network services are provided by third parties, the team communicates and coordinates with those third parties to ensure connectivity recovery. In the event of an emergency requiring migration to Evolve IP availability zones, the team ensures that all network services in the secondary availability zones are brought online once critical systems are connectivityd. Employees get connectivity in the following order: All members of the DR teams All C-Levels and Executives All remaining EMPLOYEES Install and implement all tools, hardware, software and systems required in the standby availability zone Install and implement all Hardware, software, and systems required in the primary availability zone after the organization name returns to the agenda. passes. provides the Disaster Recovery Lead with a report that summarizes emergency activity. The server team is responsible for deploying the physical server infrastructure that the organization needs to run its IT operations and applications in the event of an emergency and during an emergency. You are primarily responsible for providing base server functionality and can support other IT DR teams as needed. Edit this list to reflect your organization In the event of an emergency that does not require migration to/from Evolve IP availability zones, the team determines which servers in the primary availability zone are not working If multiple servers are affected, the team prioritizes restoring servers in the manner and order that has the least business impact. Recovery includes the following tasks: Evaluating server corruption Restart and update servers as needed to ensure that secondary servers in Evolve IP availability zones are kept up-to-date with system patches Ensure that secondary servers in Evolve IP availability zones with application patches are kept up-to-date. Keep IP availability zones up-to-date in Evolve, with data copies ensure that the secondary servers in the standby availability zones are secured appropriately, Ensure that all servers in the standby availability zones comply with the organization name server policy and install and implement all the tools, hardware, and systems needed in the standby availability zones, and implement all the tools, hardware, and systems required in the primary availability zones after the organization name works as usual. This team will summarize all costs and provide the disaster recovery lead with a report that summarizes its activities during the emergency. The application team is responsible for ensuring that all organizational applications work as needed to meet business goals in the event of a disaster and disaster. They are primarily responsible for ensuring and validating appropriate application performance and can help other IT DR teams when needed. Edit this list to reflect your organization In the event of an emergency that does not require migration to/from Evolve IP availability zones, the team determines which applications in the primary availability zones will not work If multiple applications are affected, the team prioritizes restoring applications in the manner and order that has the least business impact. The recovery includes the following tasks: Evaluating the on Application Processes, restart applications as needed, re-encode applications as needed, or rewrite to ensure that secondary servers in Evolve IP availability zones with application patches are kept up-to-date with application patches. Be. Implement all the tools, software, and patches required in the standby availability zones Install and implement all the tools, software, and patches required in the primary availability zones After the organization name works as usual, this team will summarize all costs and provide the Disaster Recovery Lead with a report that summarizes its activities during the emergency. This section explains where all of the organization's data is located and where it is backed up. Use this information to find and recover data in an emergency. In this section, it is important to explain where the organization's data is located. Discuss the location of all servers, backups, and external backups in your organization, and list what information is stored on each of these servers. In this section, list all the data in your organization in the order of its criticality. Adjust the rows as needed. Rank Data Data Data Backup Location(s) 1 Data name or group Confidential, public, personal information Frequency that data is backed up 2 3 4 4 4 5 6 7 8 9 10 Required In case of emergency actual occurrence and organization name need to perform this plan, this section is often mentioned because it contains all the information that describes the way in which the organization name information system is restored. This section contains all the information your organization needs to return to its regular functionality after an emergency. It is important to include all standard operating procedures documents, run-books, network diagrams, software format information, and so on in this section. Current System Architecture Required Insert a detailed system architecture diagram that identifies all your systems and their locations. System Architecture Diagram Example: Please list all IT systems in your organization in order of their criticality. Next, list the components of each system that need to be brought back online in the event of a disaster. Add or delete rows to the following table as needed. Ranking IT System System Components (in order of meaning) 1 1 1 2 2 2 3 3 3 3 4 Provider Circuit Type Bandwidth CPE CPE Gear Model Address, City State ZIP Location Notes Cogent Internet 1 Gbps No 630 Allendale Rd. King of Prussia, PA 19406 Network Closet Floor 1 Rack 2 Slot 40 Primary Internet Circuit Level 3 MPLS 50 Mbps Yes Cisco 3750 630 Allendale Rd. King of Prussia, PA 19406 Network Closet Floor 1 Rack 2 Slot 38 Connection to Ohio Office Cogent Internet 10MB No 630 Allendale Rd. King of Prussia, PA 19406 Network Cabinet Floor 1 Rack 2 Slot 37 Backup Internet-Model-Make/Make Model IP Misc. Details Make/Model Description MGMT IP Misc. Details Make/Model Description MGMT IP Misc. Details Make/Model Description MGMT IP Misc. Details Make/Model Description MGMT IP Misc. Details Make/Model Description MGMT IP Misc. Details Make/Model Description MGMT IP Misc : (Rang 1 = = Important) Name Rank Type VM or PHY CPU RAM Disk OS Version Purpose When determining the correct disaster recovery services, there are three aspects to consider: source of system – whether your system is on site, in the Evolve IP Cloud or elsewhere. Recovery Point Objective (RPO) — How up-to-date your data is at the recovery site. Recovery Time Objective (RTO) – How long it should take to bring an environment back online once a disaster or major incident is reported. In this section, you must rank the components of each system by severity and provide the information each system needs to bring it back online. EXAMPLE: System Name Status of the name of the system here Servername Status of the name of the specific server here Recovery time target State the IT Component's Recovery Time Objective here Recovery Point Objective State the IT Component's Recovery Point Objective here Replication Target Site Evolve IP East / West Replication Technology DRaaS ZT Backup Target Evolve IP Cloud Backup or Reflection Backup Job Frequency Nightly Restore Test The following steps are related to the reintroduction of component name in case of an emergency. Step Action Responsibility 1 , Step 1 Action, Person/Group responsible 2 3 4 5 Repeat as above for as many systems as the organization uses. While efforts are needed to make this DR plan as complete and accurate as possible, it is essentially impossible to address all possible problems at the same time. In addition, the organization's disaster recovery requirements change over time. Because of these two factors, this plan must be tested. Maintenance Required The DR plan is updated, frequency is specified, or every time a major system update or update is performed, whichever is more common. The Disaster Recovery Lead is responsible for updating the entire document and can therefore request information and updates from other employees and departments within the organization to complete this task. Maintenance of the plan includes (but is not limited to) the following: Edit this list as needed To ensure that all team lists are up-to-date to ensure that all statements remain relevant to the organization. When a member of a disaster recovery team no longer works with the organization, it is the responsibility of the Disaster Recovery Lead to appoint a new team member. Testing the required organization name is required to ensure that this DR plan is working. The DR plan should be tested at each display frequency to ensure that it remains in effect. Is done as follows: Choose which method(s) your organization will use to test the DR-Plan-DR sample: Team members orally go through the specific steps documented in the plan to confirm effectiveness, identify gaps, bottlenecks, or other weaknesses. This test provides the ability to review a plan with a larger subset of people so that the DR plan manager can make appropriate changes to the plan. Employees should be familiar with the procedures, equipment, and all Evolve IP availability zones (if necessary). Failover tests: In this scenario, servers and applications are brought online in an isolated environment. There is no impact on existing operations or uptime. System administrators ensure that all operating systems are properly available. Application administrators verify that all applications are running as expected. Live failover tests: A live failover test activates the entire DR plan. The test will interfere with normal operation and should therefore be approached with caution. Make sure that you have completed multiple iterations of steps 1 and 2 before proceeding with this step. Also, communicate any expected interruptions in time before performing this test. All gaps in the DR plan discovered in the above phases are addressed by the Disaster Recovery Lead and any resources it needs. The DR lead is responsible for filling out and signing this form for each restored process. Please use a separate form for each restored business process. NAME OF BUSINESS PROCESS: Completion date of work by DR-Team ENTER DATE HERE Date of transition back to business unit management ENTER DATE HERE I confirm that the work of the disaster recovery team has been completed in accordance with the DR plan for the above process and that normal business operations have been effectively restored. DR Team Leader Name: _____ DR Team Leader Name: _____Datum: _____