

# Cis256 final project

Technology, Information Technology



Disaster recovery and business continuity plans Insert Insert The disaster recovery plan when dealing with active directory seeks to prevent reduced productivity, minimize the destruction of data and prevent interruption to the normal business routines (Rahman Mohamed, 2014). There has to be a work plan to bring back the active directory back into functionality when a failure occurs especially when forming the backbone of the organization's network. Location 1 contains the domain controller thus requires a disaster recovery plan in case of a single domain controller failure. The latter cause's failure in login and authentication. First, you need to verify if the problem is caused by the network or corruption of the AD (Rommel, 2008). It is followed performing a recovery for the directory restore thus choosing either authoritative or none. Testing then covers replication and proper functionality of domain controller.

There is the development of a lag site for replication in case there is a deletion of objects in large numbers. The aim is to keep a backup of the active directory especially at location 2. You then engage the authoritative restore. Location three will involve creating a print queue to server printers that are standalone. The list generated by the Administrator should direct the users to a print queue on the network that will allow the job to pass through even when the printer is not support by the user's workstation. Location four will establish a redundancy for the AD to carry forth replication despite the failure of domain controllers. The step is to allow for the most minimal downtime period or none especially when relating to the failure of the software or hardware in use. The administrator also uses the group policy to address alterations to passwords, security and the respective policy

as well as settings for configuration when it is critical.

Other recovery and continuity plans involve having redundancies for every role in at least one other location to cater for damages caused by natural disasters. Having multiple tapes and performing network diagnostics after a short interval of time guarantees easy detection of a problem.

#### References

Rahman Mohamed, H. (2014). A Proposed Model for IT Disaster Recovery Plan. *IJMECS*, 6(4), 57-67. doi: 10. 5815/ijmeecs. 2014. 04. 08

Rommel, F. (2008). *Active Directory disaster recovery*. Birmingham, UK: Packt Pub.