

**Data Storage and Disaster Recovery Service**  
**Office of Technology Integration (OTI)**  
**October 17, 2006**

Although hurricane season has been (thankfully) pretty quiet so far this year, we all recall the activity level and devastation of the last couple seasons and know that the exposure runs through November. With that in mind, it's probably a good time to review the university's new Information Technology Disaster Recovery and Data Backup Policy at <http://www.vpfa.fsu.edu/policies/bmanual/itdisaster.html> to make sure that all departments are in compliance. It might also be a good idea to become familiar with the new web page at <http://www.fsu.edu/prepare> which provides a comprehensive collection of resources to assist the university community in preparing and planning for a disaster.

A major initiative in the Office of Technology Integration (OTI) this past year has been the development of a remote computing capability to support the university's IT disaster recovery and business continuity efforts. The primary objective has been to leverage FSU's participation in the Florida LambdaRail (FLR), <http://www.flrnet.org>, to ensure the preservation of critical IT data and to provide a limited set of essential IT services from a remote location should a disastrous event strike the Tallahassee campus.

FLR, along with its companion network, the National LambdaRail (NLR), <http://www.nlr.net>, provide affordable bandwidth at a scale making it feasible to perform high volume network backups to a location outside of our hurricane-susceptible region. All files currently residing on OTI's centrally administered servers and storage systems are backed up to local tape resources and also to the remote site such that a version of any file can be recovered with a target recovery point of 24 hours (local resources) to 48 hours (remote site). Currently, more than 2 terabytes of files are shipped to the remote site every day.

Several departments have expressed interest in learning how they may utilize the remote site capability as part of their own disaster recovery planning initiatives. Perhaps the easiest way to ensure critical data are protected is to take advantage of a new Network Attached Storage (NAS) service offered by OTI. This storage can be made available across the campus network to any departmental server utilizing the Common Internet File System (CIFS) protocol [the Network File System (NFS) protocol is also an available option]. System administrators can effectively address the requirement for off-site disaster recovery backups simply by storing their critical data directly on the NAS device in OTI. As with other central storage systems, the NAS is backed up locally and to the remote site. The departmental administrator does not have to bother with tape backups or arrange for off-site storage. The cost of the service is \$15/Gigabyte/year.

To learn more about this new service or to find out other ways that OTI may be able to help departments with disaster recovery planning, contact Carl Baker at 644-2591 or send e-mail to [DRinfo@fsu.edu](mailto:DRinfo@fsu.edu).

*Reprint of an article in the September 8 – October 8, 2006, edition of State.*