SUBJECT: IT DISASTER RECOVERY PLAN

The District has developed a comprehensive Disaster Recovery Plan to respond to a disaster that destroys or severely cripples the District's central computer systems operated by the IT Department. The intent is to restore operations as quickly as possible with the most up-to-date available data.

The disaster recovery plan has the following primary objectives:

1. Present an orderly course of action for restoring critical computing capability to the South Huntington School District.
2. Set criteria for making the decision to recover at a cold site or repair the affected site.
3. Describe an organizational structure for carrying out the plan.
4. Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
5. Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

All disaster recovery plans assume a certain amount of risk, the primary one being how much data is lost in the event of a disaster. We recognize that the District's data recovery efforts are targeted at getting essential systems up and running with the last available off-site backups. Significant effort will be required after the system operation is restored to (1) restore data integrity to the point of the disaster and (2) to synchronize that data with any new data collected from the point of the disaster forward.

SOUTH HUNTINGTON EMPLOYEE ACCOUNT POLICY

Network Account Creation:
Network accounts are created for employees of the District upon agreeing to the South Huntington Employee Computer Services and Internet Use Regulations and Procedures. An account consists of a logon to the South Huntington network, network space to store documents, access to shared instructional network resources, and an email address in the shufsd.org domain.

Password Policy:
Passwords are an important aspect of computer security. They are the front line of protection for network access, district-wide databases and user accounts. Users are given an initial password when their account is created. They are required to change this password the first time that they log on to the network. This ensures that no one will know another user's password.

To further secure confidentiality, passwords are required to be periodically changed. Forced password changes are enforced for all users, and new passwords must be different than the current password. Staff members are responsible for taking appropriate steps to secure their passwords.

SUBJECT: IT DISASTER RECOVERY PLAN

Account Termination:
When a user leaves the district, for any reason, his/her account is disabled. The user will no longer be able to access the district's email system or network. In the event of an employee replacing a previously disabled employee, any files from the previous employee needed will be copied over to the new employee's network storage.

Adopted: 11/19/2008