OYSTERPONDS U.F.S.D. IN ORIENT
NETWORK DISASTER RECOVERY PLAN

The methodology behind the disaster recovery plan employed by the Oysterponds School District lies in a twofold ideology, Business Continuity and Risk Management.

Business Continuity

This is based on the short term requirement of post disaster operations. This section creates a logistical plan for recovery and restoration of partial or total interruption of mission critical functions within the organization. These mission critical functions are defined as:

1. Communications Link – getting information out on what has happened/happening
2. Access and use of financial management system
3. Access to network resources, files and records
4. Access to student records including legacy grades

These critical functions have been categorized in order of importance, as they are needed to continue operation in the event of a failure. The primary concern in the event of a total interruption of services would be to re-establish a communication link and allow access to financial systems to allow for the implementation of tasks necessary to repair or relocate services as needed. Once this communications infrastructure and access to financial systems has been re-established, it is the priority of district administration and the district's technology consultants, Switch Technologies, to reconnect administrative personnel with the Student Information System as quickly as possible to be ready for continuation of services as soon as a workable area is established.

Risk Management

Throughout each part of the details below, safeguards have been implemented to allow for quick recovery in the event of an emergency. Additionally, these contingencies have been installed based on a principle of bypassing risk when possible and mitigating the impact when not. In most cases shown below, potential problems which may occur already have safeguards in place to sidestep the pitfalls or bypass the outage where needed. To ensure minimized risk of file loss, all user data files are stored directly onto network drive resources and are backed-up daily.

User participation is essential to safeguard against accidental loss. ***ALL USER DATA*** files are to be stored on assigned network resources. Files not included within the network drives cannot be and ARE NOT included within this plan for disaster recovery. Users who select to stores files to their local PC's do so at their own risk without the protections afforded within this recovery plan.

Financial Management System

The district Financial Management System, **nVision**, is a server based product with workstation interfaces. This system allows for access to ALL budgetary information as well as the purchasing, employee, payroll and business functions of the district. This system, while housed in the district's primary server room, is protected through a two phase backup plan. The first and primary backup is through the districts web-based backup server. As an alternate plan, the district has a backup sent to Eastern Suffolk BOCES for offsite date storage. Either of these backups could be used to reconnect with the Finance Manager system, if needed. During a network disaster one option available to district personnel would be for them to report to Eastern Suffolk BOCES and login to their system and retrieve district data so that the business functions of the district may continue uninterrupted.

Network Data Recovery

The school district data infrastructure employs an array of technologies designed to offer the optimal performance while minimizing the possibility of down time. Based on proven financial instruction practices and standards, the Oysterponds district along with the district's technology consultants, Switch Technologies, has developed a series of backups.

The on-location backup server provides daily and weekly backup schemes to ensure safe data storage. The backup's server is located in the districts Network Operations Center and duplicated to an off-site backup server. This method safeguards against most potential concerns including fire, flood, explosion, theft, electronic invasion, vandalism or other rogue activity against the server room. By locating this central backup server in the cloud, any damage done to the physical structure housing the main server room or the servers themselves can be quickly bypassed with the introduction of new equipment in the alternate location.

Physical Setting – Risk Management

A. District Network Operation Center

The hub of district operations, this server room is located in the main hallway of the school building. This location houses all production servers and necessary communication equipment. The entire system has uninterruptible power which allows adequate time to shut down all equipment in the event of a long term power failure.

B. Off-Site Backup

Critical servers, including nVision, are backed-up to a cloud-based service with two geographically separate locations within the continental United States.

C. Student Data

The district currently uses eSchool Data Management as the student management system (SMS). This SMS is hosted by Eastern Suffolk BOCES in Holbrook and is covered by their disaster recovery plan. It is accessible from any internet connected computer. In the event that our main internet connection is not available, we can access it through our backup connection.

ADOPTED: January 14, 2020