

# Technology Backup Policy

The following policy is to be followed for backing up data within the district.

## Definitions

- **Critical Data** – Data that, if lost, will be catastrophic and/or will take many hours of manpower to recuperate from the loss. This includes the following:
  - a loss of revenue
  - compromise district legal standings
  - compromise compliance to HIPPA, GRAMA and other federal laws
  - district reporting to the state is not possible
  - compromise records which include student academic standing
  - data that may jeopardize an employee’s district standing
  - critical to maintain the day-to-day operations where if interrupted will cause grief on a district-wide basis
- **Vital Data** – Data that, if lost, will cause significant time to recover, does not meet the above definition, and if never recovered does not severely impact district business. This includes the following:
  - Data that has hard copies
  - Significant time to recover data based on retrieving from hard copies
  - Causes a delay in state reporting with not financial implications
- **Important Data** – Data that, if lost, does not impact a wide number people. This is data that typically resides at a local user level. This Data do not fall into the categories above. This includes the following
  - Work-related data
  - Data that is stored on a periodic basis...less than weekly.
- **Insignificant Data** – Data that, if lost, is not regarded as a loss to anyone.
  - Non-Work-related data

## Frequency of Backup

### Daily

All critical and vital data must be backed up daily. This includes the following:

- District Financial Data
- School Financial Data
- SIS data
- Content filtering
- School Stream
- Sub system
- Class Choice – When in use.
- Groupwise emails
- Powerschool Servers
- Alexandria
-

Includes, but not limited to the following systems

- AS400
- Sub system
- School Stream

### **Weekly**

All important data must be backed up weekly. This includes the following:

- School Servers
- Work Order systems
- Calendaring
- Web Connect
- Cognos
- Wireless configurations
- School Board Server
- Novell Server - Student and Teacher Data
- DHCP configurations
- Web Servers
- Phone Systems
- Switches and routers
- Smartr
- OSX Servers

### **Periodically**

All Important data must be backed up periodically. This includes the following

Includes but is not limited to

- Yamas controls
- Employee Data

### **Ownership**

Once a new system is assigned to the Technology department, the administrator of that new project is responsible for the backup strategy.

### **Responsibility of Disclosure**

The backup owner must inform the system stake-holders regarding backup options and strategy (no surprises). Individual owners must be informed of their backup options and strategy. Users must have the ability to save to servers or use a local backup utility.