Westbury Technology, Communications & Information Services

NOC Based Policies & Procedure

J. Marcucci, Director

I. Data Backup procedures

A. District Wide End-User Data Backup Procedures:
   • All end-users, (faculty and students) are provided a personal folder to store their data. Each school has their own file server for student and faculty data.

B. Administrative Backup Procedures:
   • All administration users personal data is stored on one server located in the IDF in the Whitehouse.
   • Finance Manager Data is backed up nightly –
     o off site through an encrypted secure VPN through Nassau BOCES
     o locally on a tape drive – tapes are swapped out daily and stored locally in a fireproof safe in the admin building

C. Student Data Backup
   • Backup through Custom Computer Services – Hauppauge
   • Backup through Infinite Campus – Minnesota through secure VPN

D. All of user data is backed up daily and stored in a fireproof safe in the HS Noc using the following schedule:
   • Full backup of all data – Saturday
   • Incremental backups – Nightly Monday through Friday
   • The retention/repeat cycle for the data is five weeks.

E. The backup server is located in High School MDF.
   • The server name is XXXXXXX. The tape device is IBM 4560SLX tape autoloader.
   • The Backup software used is Symantec Backup Exec 12.5.
   • All backup data that is stored during its retention time is located in the High School within the Tape Library holding 24 tapes at about a 186 GB each capacity.
F. Backups are checked daily by the Associate System Engineer to ensure all backup jobs were successfully completed. The ASE is responsible for storage and/or changing tapes. In the event the ASE is out the onsite technician assumes all backup responsibilities.

II. Inventory Control Procedure

A. Inventory Procedures

- The Team is responsible for maintaining records on computer networks; including hardware and software information for inventory control and upgrade purposes.

- New equipment Incoming Process:
  - All technology equipment ordered throughout the district is shipped to Receiving dock located at 4 Hitchcock Lane.
  - The Technology Director reviews and signs in all the new equipment.
  - The Technology staff then picks up the equipment, Tags the equipment, configures the equipment and enters all the relevant information into the database.- includes Sequence, dates, serial number, make/model, asset tag number, building and room numbers.

- Inventory information is submitted to the Business Office where it is sent to CBIZ – that maintains the district centralized database.
- When equipment that is replaced under RMA or warranty conditions – Inventory is updated to reflect the new serial number/ asset tag.

B. Asset Disposal – When equipment has outlived it’s usefulness, the following procedure is followed:

- Information on the equipment is gathered and sent to the Technology Director for evaluation.
- Based on the information and the recommendation of the staff, the Director compiles a list of equipment to be surplused and presents that to the Board of Education for approval.
- Once approved, the Technology department contacts the appropriate agency/company and disposes of the equipment and received certificate of destruction/wiping / etc.
- Whenever possible, the district will make every attempt to sell the equipment rather than just disposing of it.
III. **User Password Guidelines and Procedures** - All passwords have a limited life and will automatically expire forcing a renewal every 60 days

A. **Personal Accounts** – We use Active Directory for Email (Exchange) as well as User accounts. Each user is given an initial password when the account is created. The user then needs to reset the password based on the following criteria:

The rules for the new password chosen to be accepted by the system are as follows:

a. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
b. Be at least six characters in length
c. Contain characters from three of the following four categories:
   i. English uppercase characters (A through Z)
   ii. English lowercase characters (a through z)
   iii. Base 10 digits (0 through 9)
   iv. Non-alphabetic characters (for example, !, $, #, %)

Complexity requirements are enforced when passwords are changed or created. You can use an old password if it meets the rules above but we strongly suggest you chose a new one.

B. **Student Management Accounts** – Each user is given an initial password when the account is created. The user then is forced to reset the password based on the following criteria:

- **Passwords used are Case Sensitive** and stored in an encrypted
- At least eight characters in length
- Account lockout on 3 failed attempts.
- Passwords can be reset NOT retrieved

C. **Finance Manager Accounts** – Each user is given an initial password when the account is created. The user then needs to reset the password based on the following criteria:

- At least eight characters in length
- A combination of letters of mixed case, and numbers
  - Maximum password age is 60 days
  - Password must meet complexity requirements
- Account lockout on 3 failed attempts.