Password Control Standards

The Mountain Brook Schools Data Governance and Use Policy requires the use of strictly controlled passwords for network access and for access to secure sites and information. Listed below are the minimum standards that must be implemented in order to ensure the effectiveness of password controls.

Standards:

1. Users are responsible for complying with the following password standards for network access or access to secure information:
2. Passwords must never be shared with another person, unless the person is a designated security manager.
3. Every password must, where possible, be changed yearly if not more frequently.
4. Passwords must, where possible, have a minimum length of six characters.
5. When possible, for secure sites and/or software applications, user created passwords should adhere to the same criteria as required for network access. This criteria is defined in the MBS Network Group Policy Criteria for Passwords and is listed below:
    - Should NOT contain the user's account name or parts of the user's full name that exceed two consecutive characters
    - Contain characters from three of the following four categories:
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Base 10 digits (0 through 9)
    - Non-alphabetic characters (for example, !, $, #, %)
6. Passwords must never be saved when prompted by any application with the exception of central single sign-on (SSO) systems as approved by the Technology Department. This feature should be disabled in all applicable systems.
7. Passwords must not be programmed into a PC or recorded anywhere that someone may find and use them.
8. When creating a password for secure information or sites, it is important not to use are easily guessed due to their association with the user (i.e. children’s names, pets’ names, birthdays, etc…). A combination of alpha and numeric characters is more difficult to guess.

Where possible, system software should enforce the following password standards:

1. Passwords routed over a network must be encrypted.
2. Passwords must be entered in a non-display field.
3. System software must enforce the changing of passwords and the minimum length.
4. System software must disable the user password when more than five consecutive invalid passwords are given. Lockout time must be set at a minimum of 30 minutes.
5. System software should maintain a history of previous passwords and prevent their reuse.