Non-Instructional/Business Operations

SUBJECT: PASSWORD GUIDELINES

Passwords are an important way to protect the security of the District's Computer System (DCS) and maintain the integrity of sensitive or confidential data. Therefore, in order to ensure the security of the DCS, users must comply with the following:

1) Choosing Passwords

The initial password provided to a system user must be changed by the user immediately upon gaining access to the system for the first time. Passwords must contain at least eight characters, a mixture of upper and lowercase letters, special characters, and numbers. Such passwords should not be a common word, family or pet name, address, birthday, social security, or telephone number. When a password is reset, it should not duplicate the previous passwords. In addition, user accounts will lock out for thirty minutes after five unsuccessful attempts to log on to the DCS.

2) Changing Passwords

Employees of the District must change their network passwords every 60 days. Each password is secured by the individual users and maintained by the Office of Technology.

All system level passwords will be changed whenever a member of the Information Technology (IT) staff changes. All user level passwords for network access will be changed when a compromise is suspected.

3) Password Sharing

Passwords should not be shared under any circumstances. If access is required by a supervisor, the system administrator will change the user's password to permit access. When the user returns to work, the password can be reset by the user.

4) Related Security Practices

Users should log out of the DCS if they will not be returning to their workstation for a prolonged period of time. In addition, screensavers on all District computer workstations should be set to engage within thirty minutes of user inactivity. The screensaver should then require the username and password of the logged in user when returning to activity. These measures are to lessen the risk of an unauthorized person accessing an unoccupied, but still logged in, workstation. Further, users should not post their current password in plain sight of the workstation. These actions expose the DCS and the user to potential security risks and information theft.

Approved Jan. 12, 2021 by Lyncourt BOE