Book	Procedures Manual
Section	7000 Property
Title	SECURITY OF USER ACCESS TO DISTRICT TECHNOLOGY RESOURCES
Code	ap7530A
Status	Active
Adopted	October 10, 2013
Last Revised	December 10, 2015

7530A - **SECURITY OF USER ACCESS TO DISTRICT TECHNOLOGY RESOURCES**

The District recognizes the importance of maintaining the security of data and technology resources required to operate the educational enterprise. The following procedures are necessary to ensure the required security.

Authorized Users

Authorized users of the District's technology resources shall have passwords to authenticate their identity and provide access to the appropriate systems.

A. The administrator of each school or other organizational unit that uses computer equipment to communicate with the District's enterprise systems is responsible for notifying, in writing, Technology & Information Services of the names and positions of all persons who should be authorized to access data files and computer programs.

B. Appropriate persons may be properly authorized to operate computer equipment and to access enterprise system data files and computer programs, only if such operation is clearly a part of, or directly related to, the administrative workload of the school or administrative unit. In all cases they must be properly authorized (i.e. have a signed and approved security user-id agreement) when access is permitted.

C. Students, volunteers and non-school staff should not be provided access to confidential enterprise system data files and computer programs. Any exception will require prior approval of the Superintendent.

D. Technology & Information Services shall supply each duly authorized user with a unique user identification code and password to enable the user to sign on to the network.

E. All users will be required to update network passwords at least once every sixty (60) days. It shall be the responsibility of the site or department manager to require more frequent password changes according to and as appropriate for the specific duties assigned, nature of information accessed, and work location. Any site administrator, through the site tech coordinator/network administrator, may further impose restrictions at that site when a concern for access or confidentiality occurs for specific circumstances or positions. Training for site tech contacts to be able to make these adjustments independently will be provided on request or as necessary through Technology & Information Services.

F. District minimum secure password requirements are:

1. Passwords should be at least eight (8) characters, with three (3) out of four (4) of the following conditions met:

    a. must contain an uppercase letter;

    b. must contain a lowercase letter;

c. must contain a special character;

d. must contain a number.

2. The password should be changed on a regular basis and at least once every sixty (60) days where there is significant risk relating to personally identifiable confidential information being accessed.

3. New passwords should be unique in terms of those used recently.

4. Screen saver and session time-outs and monitor orientation should be set to preclude casual screen viewing by others.

G. Site Administrators shall be responsible for notifying Technology & Information Services of any change in personnel or their authorization. In particular, persons whose duties are changed so that access to computer equipment or data files is no longer required, and persons whose employment are terminated, shall be reported at once. Authorization to access enterprise system data files and computer programs may be withdrawn by the appropriate administrator at any time, by telephoning or emailing Technology & Information Services and giving the names of the employees whose authorization is to be withdrawn. However, the withdrawal of authorization must be confirmed in writing by the administrator. (The Sign On/Password Request form or email correspondence should be used for this purpose).

Each authorized user will be responsible for use of his/her assigned computer equipment. Each user must protect all data files and computer programs, by signing off the system or locking their equipment/office while unattended. The "Employee Supervisor Exit Checklist" (see link to Microsoft Word document below) or equivalent form must be completed for all employees leaving or moving to another location in the District to ensure the return of computer-related equipment items and removal of access to data files.

It is a violation of School Board policy for any person to disclose any assigned password to any other person, except to a member of the Technology & Information Services staff, for problem resolution purposes. It is the responsibility of each employee to whom a password is assigned to maintain the confidentiality of the password. Under no circumstances shall passwords be posted or kept in a place that is accessible to unauthorized persons.

In general, users shall not be given access to program libraries or to program development and productivity tools. Specific exceptions may be made by Technology & Information Services which may place additional restrictions on such access on an individual basis. Unauthorized access to program libraries and program development tools shall be considered a violation of Board policy.

All persons receiving access to the enterprise applications are responsible for obtaining appropriate training from the T&IS Training Center, for each application they are authorized to access.

For access to the form please go to http://www.forms.leon.k12.fl.us/files/employee-supervisor-exit-checklist.doc

Revised 7/16/14
Revised 10/21/15
Revised 12/10/15