POLICY 2.501

5-B I recommend that the Board approve development of the proposed new Policy 2.501, entitled "Information Security – Access Control Policy."

[Contact: Deepak Agarwal, PX 48773 and Larry Padgett, PX 48830.]

Development   **CONSENT ITEM**

- This policy sets forth access to information systems and services on the basis of business and information security requirements, as well as to meet any requirements of state or federal law. Additionally, it sets forth:

  - User IDs creations

  - Access controls for Network and servers

  - Password standards

  - Minimum access rights

  - Separation of duties

  - Periodic review of User access

  - Regulations on unattended computers

  - Controls for physical access

See Item 5A/Policy 8.123 for the referenced IT User Standards and Guidelines Manual.

POLICY 2.501

1   **INFORMATION SECURITY - ACCESS CONTROL POLICY**
2
3   1.   <u>**Purpose:**</u> <u>To control access to information. Access to information systems and</u>
4   <u>services should be controlled on the basis of business and information security</u>
5   <u>requirements as well as to meet any requirements of state or federal law. This</u>
6   <u>Policy does not prohibit or restrict public access to inspect data and information on</u>
7   <u>publicly available District technology resources.</u>

8   2.   <u>**Definitions:**</u> <u>The IT User Standards and Guidelines Manual provides definitions of</u>
9   <u>terms used within this Policy. This Manual is incorporated herein by reference as</u>
10   <u>part of this Policy and can be located on the District's IT Security web site at:</u>
11   <u>http://www.palmbeachschools.org/it/security.asp.</u>

12   3.   <u>**Policy:**</u>

13   a.   <u>User Access Management.</u>

14   i.   <u>All users, except third party users and as stated below, will be</u>
15   <u>automatically assigned a unique User ID for their use only. As to third</u>
16   <u>party users, they will be assigned a User ID, on request by their District</u>
17   <u>contact/coordinator, when in the best interest of the District. Further, all</u>
18   <u>users will have a password. Yet, as to students, see School Board Policy</u>
19   <u>8.123, sub-paragraphs (2) (d) & (e), relating to passwords and User ID's.</u>

20   ii.   <u>Access to the network/servers and information systems will be by User ID</u>
21   <u>and password and, in appropriate cases, a secondary authentication</u>
22   <u>method may be necessary, such as a smartcard, PIN number or biometric</u>
23   <u>data.</u>

24   iii. <u>IT shall utilize appropriate information system controls to enforce the</u>
25   <u>password standards defined in the IT User Standards and Guidelines</u>
26   <u>Manual.</u>

27   iv.   <u>Users will only be given sufficient rights to all systems they have been</u>
28   <u>specifically approved and authorized to use based on the District's</u>
29   <u>business and information security requirements, as well as to meet any</u>
30   <u>requirements of state or federal law. Access is also controlled by the</u>
31   <u>District's web site filtering policy—School Board Policy 8.125.</u>

32   v.   <u>User rights will be kept to a minimum at all times. Employees shall be</u>
33   <u>given, by default, basic access to e-mail and calendaring services and</u>
34   <u>appropriate self-service HR services, such as eBenefits and ePay.</u>

35   vi.   Users requiring access, other than basic, to information systems must
36   make the requests for access according to processes defined by each
37   information system owner.

38   vii. The information system owner shall be identified and will determine user
39   access rights for their systems. Information system owners shall consider
40   separation of duties when determining user access rights.

41   viii. System administration rights to information systems, including network
42   devices, shall be restricted to the appropriate users based on the
43   District's business and information security requirements.

44   ix.   The user's User ID shall be disabled when a change in his/her status,
45   such as resignation or termination, has occurred.

46   x.   User's access rights shall be periodically reviewed to make sure the
47   access is approved and authorized based on the District's business and
48   information security requirements.

49 b. Physical Access Management.

50   i.   Users must not leave their computer or other access unit unattended
51   during normal work hours without first logging off or invoking a password
52   protected screen saver.

53   ii.   Users must turn off their computers or other access units at the end of
54   normal work hours. If a computer or other access unit must stay on after
55   normal work hours, precautions shall be taken to prevent unauthorized
56   use.

57   iii. Physical access into facilities that contain information systems, such as
58   computer rooms and data storage areas, shall be restricted to those
59   people that are approved and authorized based on the District's business
60   and information security requirements. Physical access shall be
61   controlled using methods such as walls, locks, key card systems, and
62   biometric readers.

63   iv.   Physical access into controlled facilities shall be logged and monitored.

64 STATUTORY AUTHORITY: Fla. Stat. §§ 1001.32(2); 1001.41(2); 1001.42(26);
65 1001.43(1)
66 LAWS IMPLEMENTED: Fla. Stat. §§ 1001.32(2); 1001.43(3); 1001.42(8) & (9);
67 1003.31; 1006.28(1)
68 HISTORY: __/___2010

Legal Signoff:

The Legal Department has reviewed proposed Policy 2.501 and finds it legally sufficient for development by the Board.

_____   _____

Attorney   Date