



## STATE BOARD OF ADMINISTRATION

1801 Hermitage Boulevard-Suite 100  
Tallahassee, Florida 32308  
(850) 488-4406

Post Office Box 13300  
32317-3300

**JEB BUSH**  
GOVERNOR  
AS CHAIRMAN  
**TOM GALLAGHER**  
CHIEF FINANCIAL OFFICER  
AS TREASURER  
**CHARLIE CRIST**  
ATTORNEY GENERAL  
AS SECRETARY  
**COLEMAN STIPANOVICH**  
EXECUTIVE DIRECTOR

### Internal Audit Memorandum 2005-03

November 17, 2005

**Coleman Stipanovich** *CS*  
Executive Director  
State Board of Administration  
1801 Hermitage Boulevard  
Tallahassee, Florida 32308

Dear Coleman:

**RE:** PriceWaterhouseCoopers' "Information Technology Audit Observations" for SBA in Conjunction with the Florida Prepaid College Board Financial Statements Audit as of June 30, 2005.

The PriceWaterhouse Coopers (PWC) audited the SBA's Information Technology (IT) Department as part of their June 30, 2005 financial statements audit of the Florida Prepaid College Board (FPP). As a result of the audit, PWC issued a draft report titled "Information Technology Audit Observations" dated July 15, 2005. The draft report was forwarded by Bill Nichols, FPP Director of Operations, to Gwenn Thomas, Chief Operating Officer; Greg Mathes, Director of IT; and Florida D. Rivera-Alsing, Chief of Internal Audit on August 16, 2005 with a note that the draft report is for informational purposes only and no response is required. A copy of the draft report is attached as Appendix A.

We, the Office of Internal Audit, requested the IT Department to advise us of the actions taken on the recommendations contained in the draft report. The responses we received are discussed in the subsequent pages of this memorandum.

We did not endeavor to evaluate or validate the responses received. We recommend that the responses be reviewed by management to ensure that the decisions made by IT are not exposing the SBA to unnecessary risks. For the recommendations that were

## Internal Audit Memorandum 2005-03

November 17, 2005  
PWC IT Audit – July 15, 2005  
Page 2 of 4

implemented, we will perform follow-up procedures when we audit certain sections of IT as planned.

The PWC draft report contained seven audit findings categorized under System Security (windows and physical security) and Program Changes/Development. PWC findings and recommendations were captured verbatim below.

### A. System Security:

#### 1. Windows Security

PWC Finding and Recommendation:

- a. Strong passwords are not enforced through the 'Local Security Settings' password policy. Minimum password length is 5 characters. Password complexity option is not enable.

IT Response:

We were advised that the current minimum password length is 5. The complexity option is indeed not enabled.

PWC Finding and Recommendation:

- b. Account lockout threshold is set to 5 bad log-on attempts. Industry standards recommend the following configuration: Lockout after 3 bad logon attempts. Reset bad logon count after 1440 minutes. Lockout duration: 0 minutes

IT Response:

We were advised that the current invalid log-on attempts will continue to be five because it gives users an opportunity to remember a recently changed password without locking their account. The industry standard for invalid log-on lockout is between three and five. IT decided to keep it at five.

#### 2. Windows Security:

PWC Finding and Recommendation:

The following services were found to be running on Windows Server Alerter: Com+Event System running, DHCP Client, Distributed Transaction Coordinator, Error Reporting Service, Help and Support, Intersite Messaging, Kerberos Key Distribution Center Messenger, Shell Hardware Detection, System Event Notification, Task Scheduler, Windows Audio Workstation.

## Internal Audit Memorandum 2005-03

November 17, 2005

PWC IT Audit – July 15, 2005

Page 3 of 4

PWC recommended to disable all services which are not necessary for the system to operate effectively.

IT Response:

All of the services identified by the PWC auditors are deemed necessary for system functionality, system alerts, maintenance tasks, and disaster recovery.

### 3. Windows Security:

PWC Finding and Recommendation:

The following services were enabled: Automatic updates. PWC recommended that servers are updated manually by the System Administrator.

IT Response:

We were advised the updates are downloaded automatically but are installed manually by the Systems Administrator who makes the ultimate decision as to what updates to apply.

### 4. Windows Security:

PWC Finding and Recommendation:

Force shutdown from a remote system is restricted to administrators and operators. PWC recommended to remove privileges, if not necessary.

IT Response:

We were advised that the windows security remote shutdown is a privilege granted only to the Systems Administrators and Server Operators. This privilege allows remote troubleshooting of the systems in the event of a failure.

### 5. Physical Security:

PWC Finding and Recommendation:

Access to the computer room was not appropriately restricted: a) Terminated employee had access to the data center, and b) 20 individuals had access to the data center whose job function did not require access. PWC recommended to restrict computer room access to personnel who require access to perform job. PWC also recommended to perform periodic reviews of computer access.

**Internal Audit Memorandum 2005-03**

November 17, 2005  
PWC IT Audit – July 15, 2005  
Page 4 of 4

IT Response:

We were advised that the recommendation was implemented and access to the computer room was changed subsequent to the PWC IT audit.

**B. Program Changes/Development:**

PWC Finding and Recommendation:

6. Evidence of formal sign off to go live was not maintained. PWC recommended to maintain evidence of approval for going live with program changes.
7. Evidence of formal sign off by users was not maintained. PWC recommended to maintain evidence of approval by end user.

IT Response:

We were advised that both findings are related to requiring a formal sign off. We were further advised that, starting December 2004, the Applications and Development Section in IT has reinstated the use of the Application Development Review and Approval Form that requires formal sign off by the programmer, tester, user, data center management and the IT staff who moved it to the production environment.

Please let us know if you need any additional information.

Sincerely,



Florida D. Rivera-Alsing  
Chief of Internal Audit  
***Office of Internal Audit***

Enclosure-as stated

cc: Gwenn Thomas, Chief Operating Officer



# *Florida Prepaid College Plan*

## **Information Technology Audit Observations**

**\*\*\* D R A F T \*\*\***

July 15, 2005

**Florida Prepaid College Plan  
Information Technology Audit Observations - DRAFT  
July 15, 2005**

Ref#	Area	Finding	Risk	Recommendation	Management Response
<b>System Security</b>					
	<b>Windows Security</b>	<p>Strong passwords are not enforced through the 'Local Security Settings' password policy</p> <p>Account lockout threshold is set to 5 bad log-on attempts. Min password len: 5 chars Password complexity option is not enable</p>	Having a high degree of password strength decreases the likelihood of passwords being compromised.	<p>Industry standards recommend the following configuration:</p> <p>Lockout after 3 bad logon attempts Reset bad logon count after 1440 minutes Lockout duration: 0 minutes</p>	
	<b>Windows Security</b>	<p>The following services were found to be running on Windows Server</p> <ul style="list-style-type: none"> <li>Alerter</li> <li>COM+ Event System - running</li> <li>DHCP Client</li> <li>Distributed Transaction Coordinator</li> <li>Error Reporting Service</li> <li>Help and Support</li> <li>Intersite Messaging</li> <li>Kerberos Key Distribution Center</li> <li>Messenger</li> <li>Shell Hardware Detection</li> <li>System Event Notification</li> <li>Task Scheduler</li> <li>Windows Audio</li> <li>Workstation</li> </ul>	Running additional, unnecessary services increases the risk of a malicious user utilizing these services to compromise the security of the systems. Any vulnerability that exists for these services may be used to exploit the system.	Disable all services which are not necessary for the system to operate effectively.	
	<b>Windows Security</b>	<p>The following services was enabled</p> <p>Automatic Updates</p>	Running additional, unnecessary services increases the risk of a malicious user utilizing these services to compromise the security of the systems	Recommended that servers are updated manually by the System Administrator	

**Florida Prepaid College Plan  
Information Technology Audit Observations - DRAFT  
July 15, 2005**

Ref#	Area	Finding	Risk	Recommendation	Management Response
	<b>Windows Security</b>	Force shutdown from a remote system' is restricted to administrators and operators, Recommended no group has access.	User groups granted inappropriate privileges can severely increase the risk of a compromise in security	If not needed, remove privileges.	
	<b>Physical Security</b>	Access to the computer room was not appropriately restricted.  1 Terminated Employee had access to the data center.  20 Individuals had access to the data center whose job function did not require access.	Risk of entry into the computer room by personnel who do not require access to perform job. Increased risk of inadvertent or malicious acts by personnel.	Restrict computer room access to personnel who require access to perform job.  Perform periodic reviews of computer access.	
<b>Program Changes / Development</b>					
	<b>Go Live</b>	Evidence of a formal sign off to go-live was not maintained	No accountability for changes moved into production.	Maintain evidence of approval for going live with program changes	
	<b>User Acceptance Testing</b>	Evidence of a formal sign off by users were not maintained	Changes made may not meet the requirements of the end users	Maintain evidence of approval by end user	