



AUDITOR GENERAL

DAVID W. MARTIN, CPA



PASCO-HERNANDO COMMUNITY COLLEGE

Operational Audit

SUMMARY

Our operational audit for the fiscal year ended June 30, 2008, disclosed the following:

Finding No. 1: The College did not conduct a review and evaluation of social security numbers it collected or notify individuals of the purpose for collection of the numbers, contrary to Section 119.071(5)(a), Florida Statutes.

Finding No. 2: The College had not developed an ongoing information technology (IT) security awareness program to periodically remind personnel of the importance of preserving the integrity, confidentiality, and availability of data and IT resources entrusted to them.

Finding No. 3: The College lacked written policies and procedures for certain IT functions.

Finding No. 4: Certain security controls relating to user authentication needed improvement.

Finding No. 5: Certain application access and authorization controls needed improvement.

BACKGROUND

The College is under the general direction and control of the Florida Department of Education, Division of Community Colleges, and is governed by State law and State Board of Education rules. A board of trustees governs and operates the College. The Board constitutes a corporation and is composed of nine members appointed by the Governor and confirmed by the Senate. The Board members and President

who served during the audit period are listed in Exhibit A.

Pasco-Hernando Community College has campuses in Dade City (East Campus), Brooksville (North Campus), and New Port Richey (West Campus), Florida, and a center in Spring Hill, Florida. Additionally, credit and noncredit classes are offered in public schools and other locations throughout Pasco and Hernando Counties. The College reported enrollment of 5,521.9 full-time equivalent students for the 2007-08 fiscal year.

The results of our financial audit of the College for the fiscal year ended June 30, 2008, will be presented in a separate report. In addition, the Federal awards administered by the College are included within the scope of our Statewide audit of Federal awards administered by the State of Florida and the results of that audit, for the fiscal year ended June 30, 2008, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Collection of Social Security Numbers

The Legislature has acknowledged in Section 119.071(5)(a), Florida Statutes, the necessity of collecting social security numbers (SSNs) for certain purposes because of their acceptance over time as a unique numeric identifier for identity verification and

other legitimate purposes. The Legislature has also recognized that SSNs can be used to acquire sensitive personal information, the release of which could result in fraud against individuals or cause other financial or personal harm. Therefore, public entities are required to provide extra care in maintaining such information to ensure its confidential status.

Effective October 1, 2007, Section 119.071(5)(a), Florida Statutes, as amended by Chapter 2007-251, Laws of Florida, provides that an agency may not collect an individual's SSNs unless the agency has stated in writing the purpose for its collection and unless it is specifically authorized by law to do so or imperative for the performance of that agency's duties and responsibilities as prescribed by law. Additionally, this Section requires that an agency collecting an individual's SSNs provide that individual with a copy of the written statement indicating the purpose for collecting the number. Further, this Section provides that SSNs collected by an agency not be used for any purpose other than the purpose provided in the written statement. This Section also requires that each agency review whether its collection of SSNs is in compliance with the above requirements; immediately discontinue the collection of SSNs for purposes that are not in compliance; and certify to the President of the Senate and the Speaker of the House of Representatives its compliance with these requirements no later than January 31, 2008.

The College collects SSNs from students, employees and prospective employees, and certain contracted vendors for record-keeping and withholding taxes. While the College assigned student and employee ID numbers to replace using SSNs for record keeping purposes, it continued to obtain SSNs from employees, prospective employees, students, and certain contracted vendors.

Our review disclosed that, the College submitted the certification of its compliance with the requirements to the President of the Senate and the Speaker of the House of Representatives on January 23, 2008. However, the College did not conduct the required

review and evaluation of SSNs collected or prepare written statements notifying individuals of the purpose for collection of their numbers, contrary to Section 119.071(5)(a), Florida Statutes. Effective controls to properly monitor the need for and use of SSNs and ensure compliance with statutory requirements reduce the risk that SSNs may be used for unauthorized purposes.

Subsequent to our inquiries, College management indicated that the College has initiated actions to comply with the requirements of Section 119.071(5)(a), Florida Statutes.

Recommendation: The College should continue its efforts to ensure compliance with Section 119.071(5)(a), Florida Statutes. In those instances in which the College determines that collection of the social security number is not imperative for performance of its duties and responsibilities, the College should discontinue obtaining such numbers.

Finding No. 2: Security Awareness and Training

Security awareness by employees is important to minimize misuse of information technology (IT) resources. A security awareness program is designed to inform personnel of the importance of information handled and the legal and business reasons for maintaining its integrity, confidentiality, and availability. Employees must be aware of their responsibilities and the steps the organization is willing to take to ensure security through documentation describing security policies and procedures and acknowledgements of an individual's responsibility.

During our audit period, the College provided security awareness training during new employee orientation including providing the new employee a handbook which included copies of various IT policies and procedures, and requiring the employee to sign a form acknowledging receipt of the handbook. However, the College did not have a security training program in

place to facilitate employees' ongoing awareness education and training on security responsibilities. The absence of an ongoing security awareness program could jeopardize the integrity, confidentiality, and availability of system resources through the lack of users' knowledge regarding their responsibilities for the safeguarding of the College's data and IT resources.

Recommendation: The College should develop an ongoing security awareness training program to periodically remind all who use the College's computer system of the security risks and to reinforce adherence to the College's policies and procedures. Additionally, procedures should require employees to provide written acknowledgement that they read, understand, and accept the College's security awareness policies.

**Finding No. 3: Information Technology –
Written Policies and Procedures**

Each IT function needs complete, well-documented policies and procedures to describe the scope of the function and its activities. Sound policies and procedures provide benchmarks against which compliance can be measured and contribute to an effective control environment.

Our audit disclosed that the College lacked written policies and procedures for the following IT functions:

- Administration of user identification codes (IDs), vendor-supplied IDs, guest accounts, and security devices (such as routers and firewalls).
- Denial of administrator rights on workstations used by end users.
- Provision of least privilege for user access based on job function.
- User password reset, including positive identification of the user.

- Determining compliance with existing password policies.

Without written policies and procedures the risk is increased that IT controls may not be followed consistently and in a manner pursuant to management's expectations.

Recommendation: The College should establish written policies and procedures to document management's expectations for the performance of the above-listed IT functions.

**Finding No. 4: Information Technology –
Security Controls**

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain security controls relating to user authentication that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising College data and IT resources. However, we have notified appropriate College management of the specific issues. Without adequate security controls over user authentication, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that College data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The College should improve security controls in the area of user authentication to ensure the continued confidentiality, integrity, and availability of College data and IT resources.

**Finding No. 5: Information Technology –
Application Access and
Authorization Controls**

Application access and authorization controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain application access and authorization controls that needed improvement. We are not

disclosing specific details of the issues in this report to avoid the possibility of compromising College data and IT resources. However, we have notified appropriate College management of the specific issues. Without adequate application access and authorization controls, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that College data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: The College should improve application access and authorization controls to ensure the continued confidentiality, integrity, and availability of College data and IT resources.

PRIOR AUDIT FOLLOW-UP

The College had taken corrective actions for findings included in our report No. 2007-091.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this operational audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this operational audit were to: (1) obtain an understanding and make overall judgments as to whether College internal controls promoted and encouraged compliance with applicable laws, rules,

regulations, contracts, and grant agreements; the economic and efficient operation of the College; the reliability of records and reports; and the safeguarding of assets; (2) evaluate management's performance in these areas; and (3) determine whether the College had taken corrective actions for findings included in our report No. 2007-091. Also, pursuant to Section 11.45(7)(h), Florida Statutes, our audit may identify statutory and fiscal changes to be recommended to the Legislature.

The scope of this operational audit is described in Exhibit B. Our audit included examinations of various records and transactions (as well as events and conditions) occurring during the 2007-08 fiscal year.

Our audit methodology included obtaining an understanding of the internal controls by interviewing College personnel and, as appropriate, performing a walk through of relevant internal controls through observation and examination of supporting documentation and records. Additional audit procedures applied to determine that internal controls were working as designed, and to determine the College's compliance with the above-noted audit objectives, are described in Exhibit B. Specific information describing the work conducted to address the audit objectives is also included in the individual findings.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.



David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

Management's response is included as Exhibit C of this report.

The audit team leader was Anna A. McCormick, CPA, and the audit was supervised by Janice Priolo, CPA. For the information technology portion of this audit, the audit team leader was Danielle M. Alvarez, CISA, and the supervisor was Nancy M. Reeder, CPA, CISA. Please address inquiries regarding this report to James R. Stultz, CPA, Audit Manager, by e-mail at jimstultz@aud.state.fl.us or by telephone at (850) 922-2263.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

EXHIBIT A
BOARD OF TRUSTEES AND PRESIDENT

Members of the Board of Trustees and President who served during the 2007-08 fiscal year are listed below:

<u>Board Member</u>	<u>County</u>
Irvin Homer, Vice-Chair to 7-16-07, Chair from 7-17-07	Hernando
Thomas Weightman, Vice-Chair from 7-17-07	Pasco
S.K. Rao Musunuru, Chair to 7-16-07	Pasco
John S. Church	Hernando
Jeanne M. Gavish	Hernando
Deborah G. Kilgore	Hernando
Judy R. Parker	Pasco
Wilton Simpson from 8-20-07	Pasco
Karen Wells to 8-19-07 (1)	Pasco
Gary L. Worthley	Pasco

Dr. Katherine M. Johnson, President

Note: (1) Board member served beyond the end of her term, May 31, 2007.

EXHIBIT B
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Information Technology (IT) policies and procedures.	Inspected the College's written IT policies and procedures to determine whether they addressed certain important IT control functions.
Program change management procedures.	Reviewed documentation supporting the College's change management methodology for requesting, approving and implementing system changes related to IT resources.
Procedures for authorizing access to IT resources.	Reviewed documentation to determine the College's process for requesting, approving, implementing, and removing system access to IT resources. Selected a sample of access privileges granted to determine whether the College properly authorized and granted application access in relation to employees' job functions.
Procedures for IT authentication controls.	Examined supporting documentation to determine whether authentication controls were configured and enforced in accordance with IT best practices.
Security awareness and training program regarding the confidentiality of information.	Examined supporting documentation relating to the College's IT security awareness and training program.
Procedures to timely prohibit terminated employees' access to electronic data files.	Sampled employees who terminated during the audit period and examined supporting documentation evidencing when the College terminated access privileges.
Fraud policy and related procedures.	Examined written policies, procedures, and supporting documentation relating to the College's fraud policy and related procedures.
Sunshine Law requirements for Board meetings (i.e., proper notice of meetings, ready access to public, maintain minutes).	Read Board minutes and, for selected Board meetings, examined supporting documentation evidencing compliance with Sunshine Law requirements.
Tuition and technology fees.	Compared tuition and technology fees assessed to amounts authorized by law and administrative rules.
Student activity and service fees assessed.	Verified that the activity and service fee assessed did not exceed 10 percent of the total tuition fee.
Procedures for calculating user and laboratory fees.	Selected a sample of user and laboratory fees and examined supporting documentation to determine whether the College properly calculated these fees.
Adult general education program enrollment reporting.	Selected a sample of adult education students and examined supporting documentation to determine whether the College reported instructional and contact hours in accordance with FDOE requirements.

EXHIBIT B (Continued)
AUDIT SCOPE AND METHODOLOGY

Scope (Topic)	Methodology
Social security number requirements of Section 119.071(5)(a), Florida Statutes.	Examined supporting documentation to determine whether the College had provided individuals with a written statement as to the purpose of collecting social security numbers, certified compliance pursuant to 119.071(5)(a)4.b., Florida Statutes, and filed the required report specified by Section 119.071(5)(a)9.a., Florida Statutes, no later than January 31, 2008.
Procedures for adopting and amending the budget.	Examined supporting documentation to determine whether budgets and amendments to budgets were prepared and adopted in accordance with applicable Florida Statutes and State Board of Education Rules.
Procedures for tangible personal property.	Conducted physical observation of a sample of tangible personal property to verify existence, and that records adequately documented property. Selected a sample of deleted items to determine if the College followed policies, rules, and laws for deleting.
Procedures for travel reimbursement.	Selected a sample of travel reimbursements to test for compliance with Section 112.061, Florida Statutes.
Procurement policies and procedures.	Reviewed documentation that supported the College's use of the sales tax exemption for direct purchase of materials for capital projects.
Procedures for insuring architects and engineers.	Selected a sample of significant or representative major construction projects in progress during the audit period to determine whether architects and engineers engaged during the audit period were properly selected and, where applicable, had evidence of required insurance.
Procedures for monitoring cellular telephone usage and compliance with related IRS reporting requirements.	Determined whether the College either provided for compliance with IRS substantiation requirements for cellular telephone usage or, for the most recent calendar year, reported the value of cellular telephone services provided to employees as income for those employees.

EXHIBIT C
MANAGEMENT'S RESPONSE



Office of the President

October 7, 2008

Mr. David W. Martin
Auditor General
G74 Claude Pepper Bldg.
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Martin:

The following are Pasco-Hernando Community College's responses to the preliminary and tentative findings associated with the operational audit for the fiscal year ended June 30, 2008.

Finding No. 1 Collection of Social Security Numbers (SSN)

The College concurs with the finding. As noted in the audit report, the College is now in compliance with Section 119.071(5)(a), Florida Statutes. All current employees have been provided with a copy of the College's Social Security number collection and usage notification. In addition, the College requires all new employees to acknowledge receipt of the SSN notification.

Finding No. 2 Security Awareness and Training

The College concurs with the finding. As noted in the audit report, the College does provide IT security awareness training to all new employees. The College will develop an ongoing information technology (IT) security awareness program to remind employees periodically of their IT security responsibilities. Further, the College will obtain acknowledgement that employees have read, understood, and agree to abide by the College's IT security rules and procedures.

Finding No.3 Information Technology – Written Policies and Procedures

The College concurs with this finding. The College has the following IT related policies and procedures: Board Rule 6Hx19-2.65 Information Security, Internal Management Memorandum (procedures) #1-10 Microcomputer – Software Rule, #1-19 Computer Use, and #1-20 Internet Use. The College will enhance these rules and procedures and develop new ones as necessary to resolve the areas of concern.

East Campus
36727 Blanton Road
Dade City, FL 33523-7599
(352) 567-6701

North Campus
11415 Ponce de Leon Blvd.
Brooksville, FL 34601-8698
(352) 796-6726

West Campus/District Office
10230 Ridge Road
New Port Richey, FL 34654-5199
(727) 847-2727

Spring Hill Center
11245 Spring Hill Drive
Spring Hill, FL 34609
(352) 688-8798

An Equal Access/Equal Opportunity Institution

Mr. David W. Martin
Page 2
October 7, 2008

Finding No. 4 Information Technology – Security Controls

The College concurs with the finding. To the extent possible, the College will implement the suggested improvements.

Finding No. 5 Information Technology – Application Access and Authorization Controls

The College concurs with this finding. To improve its existing application and authorization controls mechanisms further, the College will take measures to address the specific areas of concern.

Should you have any questions regarding the College's responses, please contact, Mr. Ken Burdzinski, Vice President of Administration and Finance at (727) 816-3412 or burdzink@phcc.edu.

Sincerely,



Katherine M. Johnson, Ed.D.
President

c: K. Burdzinski
P. Wright
B. Horn
V. Friend

