

STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2016-115
March 2016

ST. PETERSBURG COLLEGE



Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the 2014-15 fiscal year, Dr. William D. Law, Jr., served as President and the following individuals served as Members of the Board of Trustees:

Robert J. Fine, Jr., Chair from 8-19-14, Vice Chair to 8-18-14
Jeffrey Dale Oliver, Vice Chair from 8-19-14
Deveron M. Gibbons, Chair to 8-18-14
Bridgette Bello
Lauralee Westine

The audit was coordinated by Karen J. Collington, CPA. For the information technology portion of this audit, the team leader was Sudeshna Aich, CISA, and was supervised by Heidi G. Burns, CPA, CISA.

Please address inquiries regarding this report to Jaime N. Hoelscher, CPA, Audit Supervisor, by e-mail at jaimehoelscher@aud.state.fl.us or by telephone at (850) 412-2868.

This report and other reports prepared by the Auditor General are available at:

www.myflorida.com/audgen

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

ST. PETERSBURG COLLEGE

SUMMARY

This operational audit of St. Petersburg College (College) focused on selected College processes and administrative activities and included a follow-up on findings noted in our report No. 2013-025. Our operational audit disclosed the following:

Finding 1: The College did not require all exempt employees to record time worked or that supervisors document the review and approval of such time.

Finding 2: Some unnecessary information technology (IT) access privileges existed.

Finding 3: The College needs to develop a comprehensive, written IT risk assessment plan.

Finding 4: The College needs to develop and implement a comprehensive IT security awareness training program.

BACKGROUND

St. Petersburg College (College) is under the general direction and control of the Florida Department of Education, Division of Florida Colleges, and is governed by State law and State Board of Education rules. A board of trustees (Board) governs and operates the College. The Board constitutes a corporation and is composed of five members appointed by the Governor and confirmed by the Senate. The College President serves as the executive officer and the corporate secretary of the Board, and is responsible for the operation and administration of the College.

The College has campuses in Clearwater, Seminole, St. Petersburg, and Tarpon Springs, Florida. Additionally, credit and noncredit classes are offered in public schools and other locations throughout Pinellas County. The College reported enrollment of 20,784 full-time equivalent students for the 2014-15 fiscal year.

This operational audit focused on selected College processes and administrative activities and included a follow-up on findings noted in our report No. 2013-025. The results of our financial audit of the College for the fiscal year ended June 30, 2015, 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, 2015, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Finding 1: Payroll Processing – Time Records

Effective internal controls require supervisory approval of time worked and leave used by employees to ensure that compensation payments are appropriate and leave balances are accurate. The College pays exempt employees (i.e., Career Service Salary and Administrative and Professional employees and

faculty) on a payroll-by-exception basis whereby employees are paid a fixed authorized gross amount for each payroll cycle unless the amount is altered. A payroll-by-exception methodology assumes, absent any payroll action to the contrary, that an employee worked or used available accumulated leave for the required number of hours in the pay period.

During the 2014-15 fiscal year, the College reported salary costs of \$65.1 million for exempt employees. According to College personnel, supervisory personnel monitor exempt employees' work efforts and review and approve employee leave forms. However, the College did not require exempt employees to prepare time sheets or other records to document their time worked. Without such records and supervisory review and approval of the records, there is limited assurance that exempt employee services were provided consistent with Board expectations. In addition, without appropriate records of time worked and supervisory review, there is an increased risk that employees may be incorrectly compensated and employee leave balances may not be accurate.

College records indicate that, as of May 2015, the College implemented procedures for the supervisory review and approval of records of Administrative and Professional staff time worked. College personnel also indicated that, as of January 2016, procedures were being implemented for reviewing and approving time worked for Career Service Salary staff and faculty.

Recommendation: The College should continue efforts to ensure that all exempt employees report their time worked and supervisors document the review and approval of such time.

Finding 2: Information Technology – Access Privileges

Access controls are intended to protect data and information technology (IT) resources from unauthorized disclosure, modification, or destruction. Effective access controls provide access to IT resources based on a demonstrated need to view, change, or delete data and restrict the performance of functions that are inconsistent with assigned responsibilities.

Our test of selected access privileges to the College's network and the supporting infrastructure for the Enterprise Resource Planning system disclosed some administrator access privileges that were unnecessary. We found that 15 service accounts, no longer used for College operations, had been granted administrator access privileges within the College's network domain. Administrator access privileges are typically limited to employees who are responsible for performing network administration duties or services that require complete access to network resources.

The existence of unnecessary access privileges increased the risk that unauthorized disclosure, modification, or destruction of College data and IT resources may occur. In response to our inquiry, College management indicated that the accounts would be removed.

Recommendation: The College should limit administrator access privileges to employees who are responsible for performing network administration duties or services that require complete access to network resources.

Finding 3: Information Technology – Risk Assessment

Management of IT-related risks is a key part of enterprise IT governance. Incorporating an enterprise perspective into day-to-day governance actions helps entity personnel understand the entity's greatest security risk exposures and determine whether planned controls are appropriate and adequate to secure IT resources from unauthorized disclosure, modification, or destruction. IT risk assessments, including the identification of risks, the evaluation of the likelihood of threats, and the severity of threat impact, helps support management's decisions in establishing cost-effective measures to mitigate risk and, where appropriate, formally accepting residual risk.

Although College management performed risk assessments on a defined scope or a project-by-project basis and contracted with a vendor to scan Internet facing and critical systems for vulnerabilities on a weekly or monthly basis, the College had not developed a written, comprehensive IT risk assessment. A written, comprehensive IT risk assessment would consider, in addition to network vulnerability assessments, threats and vulnerabilities at the College, system, and application levels. A written, comprehensive IT risk assessment would also document the range of risks that College's systems and data may be subject to, including those posed by internal and external users, as well as plans for the mitigation of identified risks.

In response to our inquiry, College personnel indicated that they believed their current procedures were adequate. However, the absence of a written, comprehensive IT risk assessment may lessen the College's assurance that all likely threats and vulnerabilities have been identified, the most significant risks have been addressed, and appropriate decisions have been made regarding which risks to accept and which risks to mitigate through appropriate security controls.

Recommendation: The College should develop a written, comprehensive IT risk assessment plan to provide a documented basis for managing IT-related risks.

Finding 4: Information Technology – Security Awareness Training Program

A comprehensive security awareness training program appraises new employees of, and reemphasizes to other employees, the importance of preserving the confidentiality, integrity, and availability of data and IT resources entrusted to them. Significant nonpublic records (e.g., student record information and other records that contain sensitive and confidential information) are included in the data maintained by the College's IT systems.

College employees are required to participate in a security awareness training class or video-streamed presentation at least once during employment or at the time of employee orientation. In addition, the College offered security awareness training during a professional development day held for College employees; however, the training was not mandatory. Also, College personnel indicated that cybersecurity articles are published in the College employee online magazine along with links to videos and other training materials. However, College management had not developed a security awareness training program to facilitate all employees' ongoing education and training on security responsibilities.

In response to our inquiry, College personnel indicated that they believed their current procedures were adequate. However, the absence of an ongoing security awareness training program increases the risk

that the College's employees may not be aware of the importance of the information being handled and their responsibilities for maintaining the confidentiality, integrity, and availability of College data and IT resources.

Recommendation: The College should enhance procedures to develop and implement a comprehensive security awareness training program.

PRIOR AUDIT FOLLOW-UP

The College had taken corrective actions for the findings included in our report No. 2013-025.

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 from March 2015 to January 2016 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:

- Evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines.
- Examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, reliability of records and reports, and safeguarding of assets, and identify weaknesses in those controls.
- Determine whether management had taken corrective actions for findings included in our report No. 2013-025.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

This audit was designed to identify, for those programs, activities, or functions included within the scope of the audit, weaknesses in management's internal controls; instances of noncompliance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the program, activity, or function; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of records and transactions. Unless otherwise indicated in this report, these records and transactions were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of management, staff, and vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting our audit we:

- Reviewed College written information technology (IT) policies and procedures to determine whether they addressed certain important IT control functions such as security, systems development and maintenance, and disaster recovery.
- Reviewed College procedures for maintaining and reviewing access to IT resources to determine the appropriateness and necessity of the access based on employees' job duties and user account functions and whether the access prevented the performance of incompatible duties. We also examined the administrator account access privileges granted and procedures for oversight of administrator accounts for the network, operating system, database, and application to determine whether these accounts had been appropriately assigned and managed. Specifically, we:
 - Reviewed the appropriateness of all administrative accounts for the operating system that supports the enterprise resource planning (ERP) finance and human resource (HR) application databases (32 accounts).
 - Reviewed the appropriateness of the data base administrator roles for the ERP finance (2 accounts) and HR (2 accounts) application databases.
 - Reviewed the appropriateness of administrator access privileges assigned for the ERP finance (3 accounts) and HR (4 accounts) applications.
 - Reviewed the appropriateness of access privileges granted for all employees to selected critical ERP finance application functions (3 accounts) and (6 functions).
 - Reviewed the appropriateness of access privileges granted for all employees to selected critical ERP HR application functions (8 accounts).
 - Reviewed the appropriateness of administrator access privileges for the network (75 accounts) and operating system supporting the ERP application and Web servers (24 accounts).
- Evaluated College documentation for IT authentication controls to determine whether such controls were configured and enforced.

- Evaluated IT activity procedures and reports for capturing and reviewing system activity to ensure the appropriateness of access to, and modification of, sensitive or critical resources.
- Evaluated the College's written security policies and procedures governing the classification, management, and protection of sensitive and confidential information.
- Evaluated the College's comprehensive IT disaster recovery plan to determine whether it was designed properly, operating effectively, and had been recently tested.
- Determined whether a written, comprehensive IT risk assessment had been developed to document the College's risk management and assessment processes and security controls intended to protect the confidentiality, integrity, and availability of data and IT resources.
- Determined whether an adequate comprehensive IT security awareness and training program was in place.
- Examined Board, committee, and advisory board minutes to determine whether Board approval was obtained for policies in effect during the 2014-15 fiscal year and for evidence of compliance with Sunshine Law requirements (i.e., proper notice of meetings, meetings readily accessible to the public, and properly maintaining meeting minutes).
- Examined College records to determine whether the College informed students and employees at orientation and on its Web site of the existence of the Florida Department of Law Enforcement sexual predator and sexual offender registry Web site and the toll-free telephone number that gives access to sexual predator and sexual offender public information as required by Section 1006.695, Florida Statutes.
- Examined College records to determine whether the College had developed an anti-fraud procedure to provide guidance to employees for communicating known or suspected fraud to appropriate individuals. Also, we determined whether the College had implemented appropriate and sufficient procedures to comply with its anti-fraud procedure.
- Analyzed the unencumbered balance in the unrestricted current fund of the College Board of Trustees' approved operating budget to determine whether the balance was below 5 percent of the total available fund balances at June 30, 2015. We also performed analytical procedures to determine whether financial transactions in other funds may require resources from unrestricted funds that would cause a significant reduction in available unrestricted current or auxiliary funds.
- Evaluated College policies and procedures related to electronic funds transfers to determine whether adequate controls over electronic funds transfers had been established.
- From the population of 25 payments and transfers totaling \$203,472, made by the College to its direct-support organizations during the 2014-15 fiscal year, examined College records supporting 10 selected transactions totaling \$191,030 to determine if the payments and transfers were authorized by Section 1004.70(1)(a)2 and (3), Florida Statutes.
- Selected 30 student receivables totaling \$157,630 from the population of 7,249 student receivables totaling \$3.2 million at June 30, 2015, and examined supporting documentation to determine whether student receivables were properly authorized, adequately documented, properly recorded, and complied with Section 1010.03, Florida Statutes, and Board Rule 6Hx23-5.27 Collection of Financial Obligations and Delinquent Accounts.
- Evaluated the effectiveness of the College's controls to ensure that students who had not paid fees in an approved manner were not considered in calculating full-time equivalent (FTE) enrollments for State funding purposes pursuant to Sections 1009.22(11) and 1009.23(9), Florida Statutes.
- From the population of in-State student tuition fees totaling \$47 million assessed during the 2014-15 fiscal year, examined College records related to the fees assessed for 30 selected

students to determine whether the College documented Florida residency and assessed tuition in compliance with Section 1009.21, Florida Statutes.

- Reviewed College procedures to determine whether distance learning fees totaling \$3.7 million during the 2014-15 fiscal year were assessed and collected as provided by Section 1009.23(16)(b), Florida Statutes.
- From the population of 560 industry certifications eligible for performance funding that were attained by students during the 2013-14 and 2014-15 fiscal years, selected and examined 40 certifications to determine whether the College maintained documentation for student attainment of the industry certifications.
- Selected 9 laboratory fees with revenue totaling \$702,497 from the population of 37 laboratory fees with revenue totaling \$1.3 million during the 2014-15 fiscal year, and examined College records to determine whether the fees were assessed as provided by Section 1009.23(12)(a), Florida Statutes.
- Selected four contracts that generated revenues totaling \$2.7 million from the population of ten contracts for auxiliary operations with revenues totaling \$3.3 million for the 2014-15 fiscal year, and examined College records to determine whether the College properly monitored compliance with the contract terms for fees, insurance, and other provisions. Also, we performed analytical procedures to determine whether the College's auxiliary services were self-supporting.
- Evaluated College policies and procedures regarding textbook affordability for compliance with Section 1004.085, Florida Statutes. We also examined documentation for the 22,140 textbooks added during the 2014-15 fiscal year to determine whether the textbook information was timely listed on the College's Web site.
- From the population of 3,716 employees compensated a total of \$85.4 million during the period July 1, 2014, through April 30, 2015, examined records for 30 selected employees, who were compensated a total of \$40,920 for a selected pay period, to determine the accuracy of the rate of pay and validity of employment contracts.
- Reviewed the College's policies and procedures and examined selected records for supervisory approval of time worked and leave used by noninstructional and administrative employees to evaluate whether compensation payments were appropriate.
- Reviewed the College's policies and procedures for payments of accumulated annual and sick leave (terminal leave pay) to determine whether the policies and procedures promoted compliance with State law and College policies. From the population of terminal leave payments totaling \$571,906 and made to 92 employees during the period July 1, 2014, through April 10, 2015, we examined College records supporting selected terminal leave payments totaling \$319,277 and made to 11 employees and evaluated the payments for compliance with Sections 110.122 and 1012.865, Florida Statutes, and College policy.
- Reviewed the severance pay provisions in the College President's contract to determine whether the provisions were in compliance with Section 215.425(4), Florida Statutes.
- Evaluated the College President's compensation contract for the 2014-15 fiscal year to determine whether the amounts paid did not exceed the limits established by Section 1012.885, Florida Statutes.
- Evaluated College policies and procedures for obtaining personnel background screenings and determined whether individuals in positions of special trust and responsibility, such as positions that have direct contact with persons under age 18, had undergone the appropriate background screenings.
- Reviewed College policies and procedures to determine whether health insurance was provided only to eligible employees, retirees, and dependents and that such insurance was timely canceled

upon employee termination. Also, we determined whether the College had procedures for reconciling health insurance costs to employee, retiree, and Board-approved contributions.

- Examined College records related to 11 contractual service agreements with payments totaling \$670,337, from the population of 325 consultant contracts totaling \$2.5 million during the period July 1, 2014, through March 31, 2015, to determine whether the contractors were properly selected in accordance with applicable State law and Board policy; the agreements adequately described the services to be provided and were timely executed, properly approved, and reviewed by legal staff and appropriate College management; and the contractual services payments were properly documented and adequately supported.
- From the population of 3,965 purchasing card (P-card) transactions totaling \$907,189 for the period July 1, 2014, through February 27, 2015, selected 31 P-card transactions totaling \$37,194 and examined the supporting College records to determine whether the P-card program was administered in accordance with College policies and procedures and transactions tested were not of a personal nature.
- For all 8 employees with assigned P-cards who separated from College employment during the period July 1, 2014, through March 26, 2015, examined P-card documentation to determine whether the P-cards were timely canceled upon the cardholders' separation from College employment.
- Evaluated College policies and procedures related to identifying potential conflicts of interest. For selected College officials, we reviewed Department of State, Division of Corporation, records; statements of financial interests; and College records to identify any potential relationships that represent a conflict of interest with vendors used by the College.
- Examined documentation supporting 3 payments totaling \$1.6 million related to the one major construction project in progress during the 2014-15 fiscal year with a contract amount totaling \$12.8 million and expenditures totaling \$6.2 million for the period July 1, 2014, through March 23, 2015, to determine whether the payments were in accordance with contract terms and conditions, College policies and procedures, and provisions of applicable State laws and rules. Also, we examined College records for the construction project to determine whether the College monitored the process for selecting architects, construction managers, and subcontractors.
- Reviewed two construction projects in the design phase with estimated costs of \$18.8 million to determine whether the College adequately monitored the selection of architects and construction managers.
- Selected 30 payments totaling \$1.1 million from the population of Public Education Capital Outlay (PECO) and other restricted capital outlay payments totaling \$5 million for the period July 1, 2014, through April 30, 2015, and examined supporting College records to determine whether the funds were expended in compliance with the restrictions imposed on the use of these resources.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading **MANAGEMENT'S RESPONSE**.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each College on a periodic basis. 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.



Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

St. Petersburg College



Office of the President
727-341-3241

Board of Trustees
Chairman Dale Oliver, Vice-Chair Lauralee G. Westine, Trustee Bill Foster,
Trustee Deveron M. Gibbons, Trustee Nathan Stonecipher, President William D. Law, Jr.

February 29, 2016

Sherrill F. Norman, CPA
Auditor General
111 West Madison Street
Tallahassee, Florida 32399-1450

Re: Operational Audit Responses

Dear Ms. Norman:

In response to the preliminary and tentative audit findings related to your operational audit of St. Petersburg College for the fiscal year ending June 30, 2015, we submit the attached statements of corrective action.

We wish to express our appreciation to your staff for the professional and helpful manner in which they conducted the audit.

If I can be of further assistance, please do not hesitate to call me.

Sincerely,

A handwritten signature in blue ink that reads "William D. Law Jr." in a cursive style. The signature is written over the printed name and title of the signatory.

William D. Law Jr.
President

Mailing Address: Post Office Box 13489, St. Petersburg, FL 33733-3489 • An Equal Access/Equal Opportunity institution.

Finding No. 1 Payroll Processing – Time Records: The College did not require all exempt employees to record time worked or that supervisors document the review and approval of such time.

Recommendation: The College should continue efforts to ensure that all exempt employees report their time worked and supervisors document the review and approval of such time.

Response: The College has implemented procedures to review and approve time of faculty, career service and exempt employees. The College will continue to monitor the time records process.

Finding No. 2 Information Technology – Access Privileges: Some unnecessary information technology (IT) access privileges existed.

Recommendation: The College should limit administrator access privileges to employees who are responsible for performing network administration duties or services that require complete access to network resources.

Response: The College will continue to utilize software that monitors and creates reports that provide information about Active Directory accounts and privileges.

Finding No. 3 Information Technology – Risk Assessment: The College needs to develop a comprehensive, written IT risk assessment plan.

Recommendation: The College should develop a written, comprehensive IT risk assessment plan to provide a documented basis for managing IT-related risks.

Response: The College will develop a written, comprehensive IT risk assessment. The risk assessment will include threats and vulnerabilities at the College, range of risks and plans to mitigate identified risks.

Finding No. 4 Information Technology – Security Awareness Training Program: The College needs to develop and implement a comprehensive IT security awareness training program.

Recommendation: The College should enhance its procedures to develop and implement a comprehensive security awareness training program.

Response: The College will update and implement an ongoing security awareness training program for employees. The training will be reviewed and monitored.