STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2021-052
November 2020

FLORIDA STATE COLLEGE AT JACKSONVILLE

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period January 2019 through December 2019, Mr. Kevin E. Hyde served as President of Florida State College at Jacksonville through July 14, 2019, and Dr. John Avendano served as President after that date. The following individuals served as Members of the Board of Trustees:

	County
Thomas R. McGehee Jr., Chair from 8-13-19,[a] Vice Chair through 8-12-19[b]	Duval
O. Wayne Young, Vice Chair from 8-13-19[b]	Duval
Michael M. Bell, Vice Chair from 8-13-19[b]	Nassau
Karen Bowling, Chair through 7-14-19[a]	Duval
Candace T. Holloway through 10-13-19, Vice Chair through 8-12-19[b]	Nassau
Jennifer D. Brown from 7-15-19	Duval
J. Palmer Clarkson through 8-25-19	Duval
Shantel N. Davis from 8-26-19	Duval
Laura M. DiBella	Nassau
D. Hunt Hawkins	Duval
Thomas J. Majdanics	Duval
Roderick D. Odom from 10-14-19	Nassau

[a] Chair position vacant 7-15-19, through 8-12-19.

[b] The Vice Chairs serve with equal rank and status on the Board. The purpose of the dual office is to assure leadership representation from each of the two counties served by the College.

The team leader was Dennis W. Gay, CPA, and the audit was supervised by Randy R. Arend, CPA.

Please address inquiries regarding this report to Jaime N. Hoelscher, CPA, Audit Manager, 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:

FLAuditor.gov

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

FLORIDA STATE COLLEGE AT JACKSONVILLE

SUMMARY

This operational audit of Florida State College at Jacksonville (College) focused on selected College processes and administrative activities and included a follow-up on findings noted in our report No. 2018-121. Our operational audit disclosed the following:

Finding 1: Some unnecessary information technology user access privileges existed that increase the risk that unauthorized disclosure of sensitive personal information may occur.

BACKGROUND

Florida State College at Jacksonville (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 nine 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 Jacksonville, Florida, and centers in Jacksonville and Yulee. Additionally, credit and noncredit classes are offered in public schools and other locations throughout Duval and Nassau Counties.

FINDING AND RECOMMENDATION

Finding 1: Information Technology User Access Privileges – Sensitive Personal Information

The Legislature has recognized in State law[1] that social security numbers (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. Effective controls restrict employees from accessing information unnecessary for their assigned duties and provide for documented, periodic evaluations of information technology (IT) user access privileges.

According to College personnel and records, the College established a unique identifier, other than the SSN, to identify each student and maintained student information, including SSNs, in the College IT system. Access to student SSNs should allow College employees to perform administrative, supervisory, or instructional responsibilities that serve a legitimate educational purpose in accordance with applicable State law, State Board of Education rules, and Federal law. The College collects and uses student SSNs pursuant to State law for various purposes, such as to register newly enrolled students and to comply with Federal and State requirements related to financial and academic assistance, and to perform other College responsibilities. The College indefinitely maintains records,

[1] Section 119.071(5)(a), Florida Statutes.

including SSNs, of former students who transferred, graduated, or withdrew, and of prospective students who apply for entrance into the College but did not enroll.

As of September 2020, the College's document imaging system and student records database contained sensitive personal information, including SSNs, for a total of 1,043,378 students, including 975,780 former, 45,400 prospective, and 22,198 current students. Maintenance of student SSNs for former and current students allows the College to provide student transcripts to other colleges, universities, and potential employers based on authorized requests. In addition, the College maintains records with SSNs of prospective students who apply for College admission but do not initially enroll to help determine whether students who subsequently enroll paid or needed to pay the enrollment application fee. However, the College had not established a time frame for discarding sensitive personal information of prospective students and, although we requested, College records were not provided to demonstrate a cost-benefit or risk analysis to justify the maintenance of this information indefinitely.

According to College personnel, 210 College employees had access to sensitive personal information contained in the College's document imaging system as of August 2020. In addition, based on their job duties, 119 employees, including 82 of the 210 employees with access to that information in the imaging system, had access to sensitive personal information in the College student records database.[2] College personnel indicated that periodic evaluations were conducted to monitor access to the College student records database; however, evaluations were not conducted to monitor access to the College document imaging system. Although we requested, College records were not provided to demonstrate that the 247 employees needed continuous access to the information or that occasional access could not be granted only for the time needed. According to College personnel, although the document imaging system is capable of differentiating user access privileges to former, prospective, or current student information, neither the document imaging system nor the student records database are programmed to differentiate such access and employees who had such access did not always need access to all such information to perform their duties.

In response to our inquiries, College personnel indicated that the College had implemented multi-factor authentication for records maintained in the student database system, which requires a second piece of information to verify an authorized user's identity, along with single sign-on, which allows a user to log in to multiple independent software systems with a single ID and password and verifies a user's identity through a third-party. According to College personnel, periodic evaluations of access to the document imaging system will be performed and multi-factor authentication and the single sign-on processes will be expanded to the document imaging system. Also, in March 2020 the College revised the application process to include a separate online enrollment system that avoids establishing student records containing SSNs for prospective students in the student records database until the student is actually admitted, limits the number of employees who have access to such student records, and will more readily allow for discarding applicant records when they are no longer needed or when they reach their minimum retention period.

[2] Based on their job duties, the 119 employees with access to the College student records database included, for example, employees in Finance and Student Services Departments.

The existence of unnecessary access privileges for prolonged periods increases the risk of unauthorized disclosure of sensitive personal information of students and the possibility that the information may be used to commit a fraud against College students or others.

Recommendation: The College should continue efforts to ensure sensitive student information is properly safeguarded by:

- **Periodically evaluating employee access to the document imaging system to ensure that such access is necessary based on employee job duties.**
- **Establishing a reasonable time frame for maintaining that information for prospective students who do not enroll in the College and deleting the information when the records are no longer needed or the time frame expires.**
- **Upgrading the College student records database to differentiate access privileges to former, prospective, and current student information. Additionally, if an employee only requires occasional access to sensitive personal information, access should be granted only for the time needed.**

PRIOR AUDIT FOLLOW-UP

The College had taken corrective actions for the findings included in our report No. 2018-121.

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 2020 through September 2020 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.

This operational audit focused on information technology resources and related controls; investment income; direct-support organizations; student fees; textbook affordability; compensation and other expenses; and other processes and administrative activities. For those areas, our audit objectives 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. 2018-121.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

In planning and conducting our audit, we assessed whether internal controls were significant to our audit objectives by considering the internal control integrated framework established by the Committee of Sponsoring Organizations (COSO)[3] and adapted for a government environment within the *Standards for Internal Control in the Federal Government* issued by the United States Government Accountability Office. That framework is illustrated in the following table.

COSO Internal Control Integrated Framework

Internal Control Component	Description	Underlying Principles (To be Applied by the Board and Management)
Control Environment	Standards, processes, and structures that provide the basis for carrying out internal control across the organization. Represents the foundation on which an effective internal control system is built.	• Demonstrate commitment to integrity and ethical values. • Exercise oversight responsibility. • Establish structures and reporting lines and assign authorities and responsibilities. • Demonstrate commitment to a competent workforce. • Hold individuals accountable for their responsibilities.
Risk Assessment	Management's process to consider the impact of possible changes in the internal and external environment and to consider actions to mitigate the impact. The basis for how risks will be managed.	• Establish clear objectives to define risk and risk tolerances. • Identify, analyze, and respond to risks. • Consider the potential for fraud. • Identify, analyze, and respond to significant changes that impact the internal control system.
Control Activities	Activities in the form of policies, procedures, and standards that help management mitigate risks. Control activities may be preventive in nature or detective in nature and may be performed at all levels of the organization.	• Design control activities to achieve objectives and respond to risks. • Design control activities over technology. • Implement control activities through policies and procedures.
Information and Communication	Information obtained or generated by management to support the internal control system. Communication is the dissemination of important information to help the organization meet requirements and expectations.	• Use relevant and quality information. • Communicate necessary information internally to achieve entity objectives. • Communicate necessary information externally to achieve entity objectives.
Monitoring	Periodic or ongoing evaluations to verify that the internal control system is present and functioning properly.	• Conduct periodic or ongoing evaluations of the internal control system. • Remediate identified internal control deficiencies on a timely basis.

We determined that all components of internal control and underlying principles were significant to our audit objectives.

This audit was designed to identify, for those areas included within the scope of the audit, weaknesses in management's internal controls significant to our audit objectives; 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

[3] The Committee of Sponsoring Organizations (COSO) of the Treadway Commission was established in 1985 to develop guidance in the areas of risk and control which enable good organizational governance and reduction of fraud. Pursuant to their mission, COSO developed a framework for internal control that consists of five components and 17 underlying principles.

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; identifying and evaluating internal controls significant to our audit objectives; 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 transactions, as well as events and conditions, occurring during the audit period of January 2019 through December 2019 and selected College actions taken prior and subsequent thereto. 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 applicable laws, rules, College policies and procedures, and other guidelines, and interviewed College personnel to obtain an understanding of applicable processes and administrative activities.
- Reviewed College information technology (IT) policies and procedures to determine whether the policies and procedures addressed certain important IT control functions, such as security, systems development and maintenance, disaster recovery, and incident response and recovery.
- Evaluated College procedures for maintaining and reviewing employee access to IT data and resources. We examined access privileges to the database and finance and human resources applications during the audit period for 85 of the 216 total users to determine the appropriateness and necessity of the access based on the employees' job duties and user account functions and the adequacy with regard to preventing the performance of incompatible duties.
- Evaluated College procedures that prohibit former employees' access to College IT data and resources. From the population of 41 total users with access to the finance or human resources applications who separated from College employment during the period January 2019 through May 2020, we examined the access privileges for 25 selected users to determine whether their access privileges had been timely deactivated.
- Evaluated Board security policies and College procedures for the audit period governing the classification, management, and protection of sensitive and confidential information.
- Evaluated College procedures for protecting sensitive personal information of students, including social security numbers (SSNs). Specifically, for the 247 employees who had access to sensitive personal information of students as of August 2020, we evaluated the appropriateness of and

necessity for the access privileges based on the employees assigned job duties. We also evaluated whether College procedures for maintaining student SSNs for prospective students who did not enroll in the College were reasonable and appropriate.

- Evaluated the appropriateness of the College comprehensive IT disaster recovery plan effective during the audit period and determined whether it had been recently tested.
- Reviewed operating system, database, network, and application security settings to determine whether authentication controls were configured and enforced in accordance with IT best practices.
- Examined College records to determine whether the Board had prescribed by rule, pursuant to Section 1004.70(3)(b), Florida Statutes, the conditions with which the direct-support organization (DSO) must comply in order to use College property, facilities, and personal services and whether the Board documented consideration and approval of anticipated property, facilities, and personal services provided to the DSO and the related costs.
- From the population of 28 payments totaling $379,251 made during the audit period from the College to its DSO, examined College records supporting 16 payments totaling $359,557 to determine whether the payments complied with Section 1004.70(1)(a)2., (3), and (4), Florida Statutes.
- From the population of student fees totaling $61.3 million assessed during the audit period pursuant to Section 1009.23, Florida Statutes, determined whether certain student fees totaling $16.9 million were within amounts authorized and paid into appropriate accounts to maintain accountability.
- From the population of 6,915 course sections offered for the Summer 2018, Fall 2018, Spring 2019, and Fall 2019 Terms, examined College records supporting textbook adoptions to determine whether College textbook affordability procedures complied with Section 1004.085, Florida Statutes.
- From the population of compensation payments totaling $87,099,136 made to 3,287 employees during the audit period, selected payments totaling $51,024 made to 30 employees and examined College records supporting the payments to determine the accuracy of the rate of pay, the validity of employment contracts, whether performance evaluations were completed, the accuracy of leave records, and whether supervisory personnel reviewed and approved employee reports of time worked.
- Evaluated Board policies and College 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 Board policies. Specifically, from the population of 151 employees who separated from College employment and were paid $1,315,901 for terminal leave during the audit period, we selected 25 employees with terminal payments totaling $787,758 and examined the supporting records to determine compliance with Sections 110.122 and 1012.865, Florida Statutes, and Board policies.
- Examined severance pay provisions in College employment contracts for the President and administrative and professional employees to determine whether the provisions complied with Section 215.425(4)(a), Florida Statutes.
- Evaluated Board policies and College procedures for obtaining personnel background screenings to determine compliance with Section 1012.8551, Florida Statutes, and reviewed College records to determine whether background screenings for contractor workers and volunteers with direct contact with persons under age 18 were obtained in accordance with College procedures.
- Examined College records for the audit period to determine whether selected expenses were reasonable, correctly recorded, and adequately documented; for a valid College purpose; properly

authorized and approved; and in compliance with applicable laws, contract terms, and Board policies. Specifically:

  - From the population of general expenses totaling $97,079,634, we examined documentation relating to 30 selected payments for general expenses totaling $1,139,063.
  - From the population of contracted services expenses totaling $19,676,036, we examined documentation relating to 30 selected payments for contracted services totaling $3,185,820.

- Reviewed Board policies and College procedures related to identifying potential conflicts of interest. We also researched Department of State, Division of Corporations, records; statements of financial interests; and, from the 103 College officials (President, Trustees, and Administrative employees) and 54 non-administrative finance and purchasing employees during the audit period, selected and reviewed College records for 27 College officials and 10 non-administrative finance and purchasing employees to identify any relationships that represented a potential conflict of interest with vendors used by the College.
- From the population of 1,637 adult general education instructional students reported for 149,645 contact hours for the Fall 2019 Semester, examined College records supporting 1,829 reported contact hours for 35 selected students to determine whether the College reported the instructional contact hours in accordance with the Florida Department of Education requirements.
- From the population of 681 industry certifications reported for performance funding that were attained by students during the 2018-19 fiscal year, examined 30 industry certifications to determine whether the College maintained documentation for student attainment of the industry certifications.
- Determined whether the Board established appropriate investment policies and procedures and whether College investments during the audit period complied with those policies and procedures. Also, we determined whether any investment income was properly allocated to the funds that generated the investment income.
- Determined whether the College's unencumbered balance in the general fund was below the threshold established in Section 1011.84, Florida Statutes.
- 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

FSCJ Florida State College at Jacksonville

October 26, 2020

Sherrill F. Norman, CPA
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

Let me express our sincere appreciation for the professional manner in which your staff conducted the audit. The College's response to the preliminary and tentative finding to be included in the operational audit report for the fiscal year ended June 30, 2020 is below.

Finding No. 1: Information Technology User Access Privileges – Sensitive Personal Information

Recommendation: The College should continue efforts to ensure sensitive student information is properly safeguarded by:

- Periodically evaluating employee access to the document imaging system to ensure that such access is necessary based on employee job duties.
- Establishing a reasonable time frame for maintaining that information for prospective students who do not enroll in the College and deleting the information when the records are no longer needed or the time frame expires.
- Upgrading the College student records database to differentiate access privileges to former, prospective, and current student information. Additionally, if an employee only requires occasional access to sensitive personal information, access should be granted only for the time needed

Response: The College concurs with the finding, and will continue to refine its efforts to safeguard sensitive personal information.

The College just completed implementation of Multifactor Authentication for the imaging system to improve security of sensitive student information. In order to further improve security, staff is working to move the rights management from the imaging system to the College's Active Directory group management function. Once complete, the College will design a rights review process and build records retention schedules into the imaged student records.

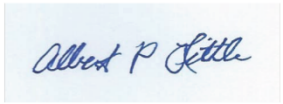
The finding referenced a large number of records of prospective students in PeopleSoft that never enrolled. The College is in the midst of moving the application process to a new system. Once complete, prospective students will no longer be created in PeopleSoft Campus Solutions until they are accepted and become active students. The new application system does not require a Social Security number. The College plans to build records retention into the new system which will purge records once they meet their scheduled timeframes and no longer have administrative value.

In response to auditor concerns during the audit, the College reviewed access rights and reduced the rights of approximately 100 staff to only see the last four digits of a student's Social Security number using a data masking tool. The same access rights review indicated that the remaining employees with rights to see sensitive student information need that access on a daily basis to successfully complete their duties. The College will continue to monitor these rights and limit access where feasible, including the possibility of temporary access should a defined role only need to view sensitive information on occasion. In addition, the annual rights review process built into PeopleSoft is being modified to inform Senior Leadership when reviews are past due.

FSCJ Florida State College at Jacksonville

Should you have any questions or concerns, please feel free to call me.

Sincerely,



Albert P. Little
Vice President, Business Services
Florida State College at Jacksonville