STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2025-052
November 2024

UNIVERSITY OF CENTRAL FLORIDA

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the 2023 calendar year, Dr. Alexander Cartwright served as President of the University of Central Florida and the following individuals served as Members of the Board of Trustees:

Alex Martins, Chair
Harold Mills, Vice Chair
Tiffany Altizer
Rick Cardenas from 1-25-23
Bill Christy
Jeff Condello
Joseph D. Conte
Danny Gaekwad
Brandon Greenaway from 6-29-23 [a]
Dr. Stephen King [b]
Daniella Lopez through 6-28-23 [a]
Caryl McAlpin
John Miklos
Michael Okaty
Beverly J. Seay through 1-24-23

[a] Student Body President.
[b] Faculty Senate Chair.

The team leader was Danielle L. Matthews, CPA, and the audit was supervised by Jeffrey M. Brizendine, 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

UNIVERSITY OF CENTRAL FLORIDA

SUMMARY

This operational audit of the University of Central Florida (University) focused on selected University processes and administrative activities and included a follow-up on findings noted in our report No. 2022-053. Our operational audit disclosed the following:

Finding 1: University personnel received an e-mail requesting a change to the payment information of a vendor and did not verify the change before electronically paying $107,625 to an incorrect bank account.

Finding 2: University procedures for periodically purging prospective students' sensitive information continued to need enhancement.

BACKGROUND

The University of Central Florida (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors (BOG). The University is directly governed by a Board of Trustees (Trustees) consisting of 13 members. The Governor appoints 6 citizen members and the BOG appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered 5-year terms. The Faculty Senate Chair and Student Body President also are members.

The BOG establishes the powers and duties of the Trustees. The Trustees are responsible for setting University policies, which provide governance in accordance with State law and BOG Regulations. The University President is selected by the Trustees and confirmed by the BOG. The University President serves as the Executive Officer and the Corporate Secretary of the Trustees and is responsible for administering the policies prescribed by the Trustees for the University.

FINDINGS AND RECOMMENDATIONS

Finding 1: Vendor Information Changes

State law[1] requires each State university to establish and maintain internal controls designed to, among other things, detect fraud, promote and encourage compliance with applicable contracts and best practices, and safeguard assets. For example, to ensure that vendor payments are appropriate and to reduce the likelihood of fraud or errors associated with those payments, it is essential for vendor information (e.g., address and bank account) changes to be properly authorized, documented, and independently verified before payments are made.

University procedures require University Finance Department personnel to enter vendor information into the University information technology (IT) System, including the specific vendor management staff who

[1] Section 1010.01(5), Florida Statutes.

are authorized to notify the University about vendor address or bank account changes. The University typically requires vendors to initiate address and bank account changes on the University Procurement Web site and provide the University with support, such as voided checks or information on bank letterhead, for bank account changes along with the account numbers. To authorize these changes, the University *Procurement Services Procedures Manual* requires the vendor management staff to authorize the changes by e-mail response to University Finance Department personnel.

University Finance Department personnel entered vendor information changes into the University IT System, which allowed payments to be made to the changed address or bank account. When entered, the Assistant Controller of Financial Affairs was prompted by the IT System to e-mail the vendor to verify the propriety of the changes. Once verified, the Assistant Controller documented approval of the changes in the University IT System. During the 2023 calendar year, University records indicated that there were 148 vendor address changes and 83 vendor bank account changes.

As part of our audit, we examined University records supporting 5 selected vendor address changes, 10 selected vendor bank account changes, and the related vendor payments. We found that University records contained documented verification that the 15 vendor information changes were appropriate. However, each of the 15 changes was immediately entered into the University IT System allowing payments to be made to the changed address or bank account before the vendor authorized the change via e-mail response. While we found that 13 of the changes were verified before a respective vendor payment was made, the University made payments to 2 vendors 47 and 36 days, respectively, before the propriety of each change was verified.

Although our test of 15 vendor information changes did not disclose fraudulent vendor address and bank account changes, the University Internal Auditor made us aware of the following sequence of events related to a fraudulent information change for a vendor that provided faculty recruiting services.

- On Friday, May 10, 2024, University Finance Department personnel received an e-mail from the vendor's e-mail address requesting the University to cancel an $84,625 check payment in progress and make an electronic payment to a new bank account. Unbeknownst to University personnel, the vendor's e-mail address had been compromised and was being used to perpetrate a fraud against the University.
- On Wednesday, May 15, 2024, University Finance Department personnel entered the information for the fraudulent bank account into the University IT System and the information was simultaneously submitted for approval to the Assistant Controller.
- On Thursday, May 16, 2024, the University canceled the $84,625 check payment in progress, plus a $23,000 check payment en route to the vendor and issued an electronic payment of $107,625 to the fraudulent bank account. That same day, the University inbox received thousands of spam e-mails (known as an "e-mail bomb") designed to overwhelm the inbox and delay detection of and response to the fraud.
- On Friday, May 17, 2024, the Assistant Controller e-mailed the vendor at 8:56 a.m. to verify the bank account change information and the vendor replied at 10:08 a.m. providing banking information that disclosed the change was not appropriate. However, possibly due to the number of spam e-mails received by the University, the Assistant Controller did not see the vendor's reply until Monday, May 20, 2024.
- On Monday, May 20, 2024, the Finance Department personnel submitted an electronic payment reversal request to the bank.

- On Wednesday, May 22, 2024, the bank returned the electronic payment reversal request because the fraudulent bank account had insufficient funds.

After the fraud occurred, in May 2024 University personnel informed the vendor that the vendor's e-mail address was used fraudulently and restored the correct vendor information into the University IT System. Also, in July 2024 the University began requiring the Assistant Controller to contact vendors by telephone to verify before approving the requested changes in the IT System.

As of September 2024, the University had recovered $2,394 of the theft. Also, during that month, the University Internal Auditor issued an investigation report about the theft, which included a timeline of the fraud scheme and several recommendations to prevent similar thefts. For example, the Internal Auditor recommended that the University:

- IT System identify vendor bank account changes as inactive until the changes are approved.
- Pursue use of a third-party to verify vendor address and bank account changes.
- Provide all finance staff with refresher training on information security incident response, identity theft, and fraud prevention and detection.

Absent effective policies and procedures over vendor address and bank account changes, the University cannot demonstrate that appropriate measures have been taken to reduce the risk of fraud and errors associated with vendor payments.

Recommendation: The University should continue efforts to ensure that, before changes to vendor information are made, the change requests are properly documented, independently verified, appropriately authorized, and reviewed.

Finding 2: Prospective Student Sensitive Personal Information

The Legislature has recognized in State law[2] 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 the confidential status of such information. In addition, University policies[3] provide that the University manage the retention and disposal of records in compliance with State regulations, including records found in the *General Records Schedules*[4] adopted by the State, which require retention periods of 5 years for certain records of students who apply for admission but are denied or who did not register.

The University collects and uses student SSNs for various purposes, such as to register newly enrolled students, comply with Federal and State requirements related to financial and academic assistance, and perform other University responsibilities. The University maintains sensitive personal records, including SSNs, for former students to provide student transcripts to universities and potential employers based on authorized requests. The University retained prospective student records indefinitely as a procedural practice for the convenience of the University and the applicant.

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

[3] University Policy 2-003 – *Records Management.*

[4] Florida Department of State, Division of Library and Information Services – *General Records Schedule GS5 for Public Universities and Colleges*, Item #97.

According to University personnel, as of February 2024 prospective student records over 5 years old had not been purged in the past 20 months due to a programming error. Subsequent to our inquiry, in March 2024 the University purged records that were over 5 years old for 379,126 prospective students, including certain records containing SSNs and other records excluding that information.[5] In May 2024, the University's Information Security Office created a standard operating procedure[6] that requires an annual process to review and purge prospective student SSNs over 5 years old from the IT System.

The existence of unnecessary access to prospective student information for prolonged periods increases the risk of unauthorized disclosure of sensitive personal information and the possibility that the information may be used to commit a fraud against University students or others. A similar finding was noted in report No. 2022-053.

Recommendation: To ensure sensitive personal information, including SSNs, of prospective students who apply but do not enroll in the University is properly safeguarded, the University should continue efforts to promptly purge information over 5 years old.

PRIOR AUDIT FOLLOW-UP

The University had taken corrective actions for findings included in our report No. 2022-053 except that Finding 2 was also noted in report No. 2022-053 as Finding 3.

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 2024 through July 2024 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 selected University 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.

[5] University records were not readily available to quantify how many of the prospective student records maintained by the University contained SSNs.

[6] SOP 714 – *Purge of Student Prospects & SSN Older Than Five Years.*

- 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. 2022-053.
- 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 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 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 the selection and examination of transactions and records, as well as events and conditions, occurring during the audit period of January 2023 through December 2023 and selected University 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, University policies and procedures, and other guidelines, and interviewed University personnel to obtain an understanding of applicable processes and administrative activities and the related requirements.
- Reviewed University information technology (IT) policies and procedures to determine whether the policies and procedures addressed certain important IT control functions, such as security access, systems development and maintenance, user authentication, and disaster recovery.

- Evaluated University procedures for maintaining and reviewing employee access to IT data and resources. Specifically, we examined access privileges to selected critical functions within the finance and human resources (HR) applications during the audit period for 77 of the 375 employees with access to those applications to determine the appropriateness and necessity of the access privileges based on the selected 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, managed, and monitored.
- Evaluated the appropriateness of the University's comprehensive IT disaster recovery plan 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.
- Determined whether a written, comprehensive IT risk assessment had been established for the audit period to document the University risk management and assessment processes and security controls intended to protect the confidentiality, integrity, and availability of data and IT resources.
- Determined whether a comprehensive IT security awareness and training program was in place for the audit period.
- Evaluated University procedures that prohibit former employees' access to University IT data and resources. Specifically, from the population of 1,451 employees who separated from University employment during the audit period, we identified the 1 employee who had access to either critical finance or HR information and determined whether the individual's access privileges were timely deactivated.
- Examined University records to determine whether the University had developed an anti-fraud policy and procedures for the audit period to provide guidance to employees for communicating known or suspected fraud to appropriate individuals. Also, we examined University records to determine whether the University had implemented appropriate and sufficient procedures to comply with its anti-fraud policy.
- Inquired whether the University had any expenses or entered into any contracts under the authority granted by a state of emergency declared or renewed during the audit period.
- Evaluated University procedures for protecting the sensitive personal information of students, including social security numbers. From the population of 1,420 employees who had access privileges to the sensitive personal information of students during the audit period, we examined University records supporting the access privileges granted to 30 selected employees to evaluate the appropriateness of and necessity for the access privileges based on the employees' assigned job responsibilities. We also determined whether the University timely purged the sensitive personal information of prospective students who applied for admission but were denied or who did not register.
- Examined University records supporting the use of the Prepping Institutions, Programs, Employers, and Learners through Incentives for Nursing Education Fund appropriation totaling $5.8 million to ensure that funding was used for eligible programs.
- Determined whether the University complied with Section 1003.64, Florida Statutes, by properly administering the Community School Grant Program and related legislative appropriation totaling $11 million and distributing funding to eligible community schools.
- Determined whether the University maintained a minimum education and general appropriation carryforward balance of at least 7 percent of its state operating budget and prepared a spending

plan for balances in excess of the 7 percent minimum balance as required by Section 1011.45, Florida Statutes.

- Reviewed University capital improvement plans for the 2022-23 and 2023-24 fiscal years to determine whether the University properly reported the capital outlay project funding sources in accordance with Board of Governors instructions for consideration in the Florida Department of Education and Capital Outlay funding submitted to the Legislature.
- From the population of 7,650 bonus and award payments totaling $18.7 million during the audit period, selected 10 payments for either performance or retention bonuses totaling $639,000 made to 10 employees and examined University records to determine whether the University complied with the requirements of Section 1012.978, Florida Statutes, and the University's Salary Administration Guidelines for Bonus and Lump Sum Payments.
- From the population of 73,119 expense card transactions totaling $29.3 million during the audit period, examined University records supporting 30 selected expense card transactions totaling $167,000 to determine whether the expense card program was administered in accordance with the *University Expense and Procurement Card Manual*, which prohibited card use to split charges to accommodate the cardholder's credit limit, and transactions were not of a personal nature.
- Examined expense card records for 30 of the 269 cardholders who separated from University employment during the audit period to determine whether the University timely canceled the cardholders' expense cards.
- Examined expense and procurement card records for 30 of the 1,883 cardholders who had active cards during the audit period to determine whether there was evidence on file that the employee accepted the card and the established conditions of card usage, and that a signed agreement form was on file for each card issued.
- Examined the effectiveness of University controls during the audit period to ensure that vendor information changes in the University information technology system are appropriate and verified.
- From the population of contracted service expenses totaling $113.2 million for the audit period, examined University records supporting 30 selected expenses totaling $8.1 million to determine whether expenses were reasonable; correctly recorded; adequately documented; for a valid University purpose; properly authorized and approved; and in accordance with applicable laws, rules, contract terms, and University policies; and whether applicable vendors were properly selected.
- From the population of student user fees collected totaling $155.8 million during the audit period, examined documentation supporting collections and conducted various audit procedures for student activity, financial aid, health, athletics, transportation, distance learning, materials and supplies, and repeat course fees totaling $112.6 million to determine whether the University properly assessed and separately accounted for the amounts as required by Section 1009.24, Florida Statutes.
- From the population of student activity fee expenses totaling $14.9 million, examined University records supporting 25 selected expenses totaling $1.9 million to evaluate University compliance with the restrictions imposed by Section 1009.24(9), Florida Statutes.
- Determined whether student financial aid fees collected totaling $13.1 million during the 2022-23 fiscal year were disbursed in compliance with Section 1009.24(7), Florida Statutes.
- Evaluated compliance with applicable use restrictions on student fees by examining University records supporting, and performing analytical procedures on, expenditures of student health, athletic, transportation, and materials and supplies fees made during the 2023 calendar year.
- From the population of 29 expense transactions totaling $1.8 million made from general revenue funds appropriated and received by the University during the audit period from the Deferred

Building Maintenance Program, examined records supporting 26 transactions totaling $1.8 million to determine whether the University expended funds pursuant to this program and the proviso language of Chapter 2022-156, Laws of Florida, General Appropriations Act, Section 197.

- From the population of two major construction projects with expenses totaling $708,000 during the audit period, selected one construction payment application totaling $100,000 related to one major construction project and examined University records to determine whether the payment was made in accordance with contract terms and conditions, University policies and procedures, and provisions of applicable State laws and rules.
- Reviewed documentation related to the two major construction projects with total construction costs of $708,000 during the audit period to determine whether the University process for selecting design professionals and construction managers was in accordance with State law; the University adequately monitored the selection process of subcontractors; the Board had adopted a policy establishing minimum insurance coverage requirements for design professionals; design professionals provided evidence of required insurance; and construction funding sources were appropriate.
- From the population of payments and transfers totaling $53.8 million made during the audit period from the University to its direct-support organizations (DSOs), examined University records supporting selected payments totaling $24.7 million and selected transfers totaling $20.9 million to determine whether the transactions were in accordance with Section 1004.28(1)(a)2. and (2), Florida Statutes.
- From the population of 105 consulting payments totaling $12 million during the audit period for new software applications, examined documentation supporting 11 selected payments totaling $7.2 million to determine whether the deliverables met the contract terms and conditions.
- 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 University 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

UNIVERSITY OF CENTRAL FLORIDA

Office of the President
P.O. Box 160002
Orlando, FL 32816-0002

November 13, 2024

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

Dear Auditor General Norman,

Thank you for the opportunity to review and respond to the preliminary and tentative findings resulting from the recent operational audit of the University of Central Florida. We appreciate the efforts of your team in evaluating our processes and procedures and highlighting areas where we can strengthen our controls and safeguard institutional resources. This audit supports our ongoing commitment to maintaining the highest standards of accountability, operational efficiency, and protection of sensitive information within our university community.

Below, please find our responses to each of the findings outlined in your report. **For Finding 1: Vendor Information Changes**, we have taken immediate steps to improve our verification protocols and ensure compliance with best practices in vendor management. Regarding **Finding 2: Prospective Student Sensitive Personal Information**, we have reinforced our data retention and purging processes to uphold the privacy and security of prospective student information.

In each area, the University is dedicated to implementing improvements and refining our procedures to mitigate potential risks, safeguard resources, and meet compliance requirements. These responses reflect our resolve to continuously improve our operational practices in alignment with both state guidelines and the University of Central Florida's institutional values.

Finding 1: Vendor Information Changes

Recommendation: The University should continue efforts to ensure that, before changes to vendor information are made, the change requests are properly documented, independently verified, appropriately authorized, and reviewed.

Management Response: Management concurs with the finding and has implemented enhanced procedures to ensure that changes to vendor banking and address information are rigorously documented, independently verified, authorized, and reviewed prior to processing. Improvements underway include updates to the Workday supplier change workflows to prevent payments from being issued until vendor information is fully verified and approved within the system. In the interim, a manual verification process is in place to mitigate risk until system updates are completed. UCF is also evaluating additional vendor management functionalities in Workday and considering third-party vendor verification services to further strengthen these processes.

Phone: 407.823.1823 • Fax: 407.823.2264

UNIVERSITY OF CENTRAL FLORIDA

To ensure awareness and adherence to these protocols, all finance staff are required to complete annual training, including UCF Information Security Awareness, Red Flags Identity Theft Prevention, and Fraud Awareness Training as part of their Workday access requirements. To reinforce these protocols, finance staff participated in refresher training on October 31, 2024, which emphasized vigilance in identifying and mitigating potential fraud risks related to financial transactions.

Finding 2: Prospective Student Sensitive Personal Information

Recommendation: To ensure sensitive personal information, including SSNs, of prospective students who apply but do not enroll in the University is properly safeguarded, the University should continue efforts to promptly purge information over 5 years old.

Management Response: Management concurs with this finding. UCF IT and Undergraduate Admissions have coordinated to schedule the upcoming annual data purge for late November to early December 2024, ensuring adherence to data retention requirements. Enhanced scheduling and notification controls have been established to reinforce communication and awareness of this annual process. Additionally, all relevant employees will receive ongoing training on SOP 714 – Purge of Student Prospects & SSNs Older Than Five Years, to reinforce the importance of timely data purging and compliance with information security standards.

The university values the insights gained through this audit and are committed to ongoing dialogue and collaboration with your office to ensure that our practices align with the highest standards of governance. Should your office have any additional questions or require further information on our corrective actions, please do not hesitate to reach out.

Thank you again for your partnership and dedication to enhancing accountability and excellence within Florida's public universities.

Sincerely,

Alexander N. Cartwright, Ph.D.
President and Professor of Electrical and Computer Engineering
University of Central Florida

Phone: 407.823.1823 • Fax: 407.823.2264