STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2021-041
October 2020

UNIVERSITY OF NORTH FLORIDA

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period January 2019 through December 2019, Dr. David M. Szymanski served as President of the University of North Florida and the following individuals served as Members of the Board of Trustees:

Kevin E. Hyde, Chair	Dr. David Fenner [b]
Sharon Wamble-King, Vice Chair	Wilfredo J. Gonzalez
John Aloszka from 4-12-19 [a]	Adam Hollingsworth
Thomas A. Bryan	Stephen C. Joost
Major General Douglas Burnett (Ret.)	Paul E. McElroy
Jenna DuPilka through 4-11-19 [a]	Oscar Munoz
Dr. Anne T. Egan	Hans G. Tanzler III

[a] Student Body President.

[b] Faculty Association President (equivalent to faculty senate chair referred to in Section 1001.71(1), Florida Statutes).

The team leader was Donald D. Hemmingway, 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

UNIVERSITY OF NORTH FLORIDA

SUMMARY

This operational audit of the University of North Florida (University) focused on selected University processes and administrative activities and included a follow-up on findings noted in our report No. 2018-130. Our operational audit disclosed the following:

Finding 1: The University made severance payments totaling $86,553 that were contrary to State law.

Finding 2: Some unnecessary information technology user access privileges existed that increase the risk that unauthorized disclosure of sensitive personal information may occur. A similar finding was noted in our report No. 2018-130.

BACKGROUND

The University of North 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 Association President and Student Body President also are members.

The BOG establishes the powers and duties of the Trustees. The Trustees are responsible for setting University regulations, 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 regulations prescribed by the Trustees for the University.

FINDINGS AND RECOMMENDATIONS

Finding 1: Severance Payments

State law[1] provides that an employee may receive severance pay that is not provided for in a contract or employment agreement if the severance pay represents the settlement of an employment dispute and the amount does not exceed 6 weeks of compensation. State law[2] defines severance pay as salary, benefits, or perquisites for employment services yet to be rendered that are provided to an employee who has recently been or is about to be terminated.

University policies[3] provide that employees may be separated from the University without cause, provided advance notice is given to the employee, or the University elects to negotiate a lump sum payment in lieu

[1] Section 215.425(4)(b), Florida Statutes.

[2] Section 215.425(4)(d), Florida Statutes.

[3] University Policy 4.0280P – *Separation From Employment*.

of providing the advance notice. The policies also provide that all non-tenured, non-unit faculty, or administrative employees as of February 2006 with more than 2 years of employment shall be given 12 months advance notice of separation and those with 2 years or less of employment shall be given 6 months advance notice. The policies further provide that those employees hired during or after February 2006 with more than 2 years of employment shall be given 90 days advance notice of separation and those with 2 years or less of employment shall be given 60 days advance notice.

During the period January 2019 through December 2019, University records indicated that two employees received lump sum severance payments totaling $86,553 based on their length of employment as of February 2006, with one employee receiving a lump sum payment of 6 months compensation (26 weeks) and the other employee receiving a lump sum payment of 12 months of compensation (52 weeks). University personnel indicated that the two employees were provided the lump sum payments and were separated from University employment pursuant to University policies in lieu of providing advance notice. In addition, the employees did not have employment contracts and there were no severance agreements or other University records evidencing the existence of an employment dispute. However, absent an enforceable employment agreement vesting employees with the right to receive severance pay or the existence of an employment dispute settlement, such payments are contrary to State law. Consequently, University records did not evidence the authority for these severance payments.

In response to our inquiries, University personnel indicated that these payments were not viewed as severance payments pursuant to State law. Instead, they believed that the payments were made in good faith to fulfill the University's prior obligations pursuant to University policies and that University policies were under revision to limit lump sum payments to the amounts permitted by law. Notwithstanding, as these payments represented compensation for employment services not yet rendered, and there was no enforceable employment agreement or employment dispute settlement, the University severance pay provisions for University employment separations without cause and related severance payments were contrary to State law.

Recommendation: The University should continue efforts to ensure that University policies and procedures limit severance pay consistent with State law.

Finding 2: Information Technology User Access Privileges – Sensitive Personal Information

The Legislature has recognized in State law[4] 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 to help prevent employees from accessing sensitive personal information inconsistent with their duties.

According to University personnel and records, the University established a unique identifier, other than the SSN, to identify each student and maintained student information, including SSNs, in the University

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

image documenting system and student records database. The University 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.

University personnel indicated that, as of July 2020, the University document imaging system and student records database contained sensitive personal information, including SSNs, for a total of 514,290 students, including 281,869 prospective, 202,047 former, and 30,374 current students. Maintenance of student SSNs for current and former students allows the University to provide student transcripts to other universities, colleges, and potential employers based on authorized requests. In addition, the University maintains records containing the SSNs of prospective students who apply for admission to the University but do not enroll to assist individuals in the application and admission process, avoid the resubmission of duplicate and sometimes costly records, and to help the University in analyzing applicant data and focusing recruitment efforts. However, the University had not established a time frame for discarding sensitive personal information of prospective students and, although we requested, University records were not provided to demonstrate a cost-benefit or risk analysis to justify the maintenance of this information indefinitely.

According to University personnel, 288 employees had access to sensitive personal information contained in the University document imaging system as of July 2020. In addition, 45 of the 288 employees with access to that information in the imaging system, along with 13 other employees, had access based on their job duties to sensitive personal information in the University student records database.[5] University personnel indicated that user access privileges require two-factor authentication, which requires a second piece of information to verify an authorized user's identity to reduce the risk of user accounts being compromised, and that periodic evaluations were conducted to monitor access to the University student records database. However, periodic evaluations were not conducted to monitor the access to the University document imaging system and, although we requested, University records were not provided to demonstrate that these employees needed continuous access to the information or that occasional access could not be granted only for the time needed. Additionally, according to University personnel, neither the document imaging system nor the student records database had a mechanism to differentiate user access privileges to prospective, former, or current student information and employees who had such access did not always need access to all such information to perform their duties.

Subsequent to our inquiries, in September 2020 University personnel indicated that employee access to the document imaging system was under evaluation and that the University would establish periodic procedures evaluating such access. However, University personnel indicated that granting and removing access privileges of employees who do not need continuous access is not worth the benefit provided even if such access was needed only once a month. Notwithstanding this response, 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 University students or others. A similar finding was noted in our report No. 2018-130.

[5] Based on their job duties, the 58 employees with access to the University student records database included, for example, employees in Enrollment Services, Financial Aid, and the Registrar Office.

Recommendation: To ensure that sensitive personal information maintained by the University is properly safeguarded, the University should:

- **Complete efforts to evaluate employee access to the document imaging system and establish procedures to periodically conduct future evaluations to ensure that such access is necessary based on employee job duties.**
- **Document the viable public purpose for maintaining that information for prospective students who do not enroll in the University, establish a reasonable time frame for maintaining the information, and delete the information when the time frame expires.**
- **Upgrade the University IT system to include a mechanism to differentiate access privileges to former, prospective, and current student information. Additionally, if an employee only requires occasional access to the sensitive personal information, the access should be granted only for the time needed.**

PRIOR AUDIT FOLLOW-UP

The University had taken corrective actions for findings included in our report No. 2018-130, except that Finding 2 was also noted in report No. 2018-130 as Finding 7.

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 February 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; public meetings and communications; carryforward balances; investment income; direct-support organizations; student fees; decentralized cash collections; 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. 2018-130.

- 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)[6] 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 and efficiency and the stewardship of management. Professional judgment has been used in determining

[6] The 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.

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 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.
- 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, user authentication, and disaster recovery.
- Evaluated University procedures for maintaining and reviewing employee access to IT data and resources. From the population of 122 employees with access to the University's database and finance or human resource applications, we examined University records supporting the access privileges for 27 employees to determine the appropriateness and necessity of access privileges based on employees' job duties and user account functions and whether incompatible duties were prevented.
- Evaluated University procedures that prohibit former employees' access to University IT data and resources. We examined the access privileges for the 26 former employees who separated from University employment and who had access to the University's database and finance or human resource applications to determine whether their access privileges had been timely deactivated.
- Evaluated University procedures for maintaining and protecting the sensitive personal information of students, such as social security numbers (SSNs). Specifically, for the 301 employees who had access to student SSNs as of July 2020, we evaluated the appropriateness of and necessity for the access privileges based on the employees' assigned job duties. We also evaluated whether University procedures for maintaining student SSNs for prospective students who did not enroll in the University were reasonable and appropriate.

- 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 Board of Trustees, committee, and advisory board meeting minutes and other records to determine whether Trustee approval was obtained for the University policies and procedures in effect during the audit period and for evidence of compliance with Sunshine Law requirements (i.e., proper notice of meetings, meetings readily accessible to the public, and properly maintained meeting minutes).
- Examined University records supporting the 144 payments and transfers, totaling $2 million, made from the University to its direct-support organizations during the audit period to determine whether the payments complied with Section 1004.28(2), Florida Statutes.
- Examined University records to determine whether the Trustees had prescribed by regulation, pursuant to Section 1004.28(2)(b), Florida Statutes, the conditions with which the direct-support organizations (DSOs) must comply in order to use University property, facilities, and personal services and whether the Trustees documented consideration and approval of anticipated property, facilities, and personal services provided to the DSOs and the related costs.
- Reviewed University records supporting textbook adoptions for 2,635 and 2,491 course sections offered during the Fall 2018 and Spring 2019 Terms, respectively, to determine whether the University textbook affordability procedures complied with Section 1004.085, Florida Statutes.
- Determined whether the University maintained a minimum 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.
- Examined University records to determine whether investment accounts maintained during the audit period were timely reconciled to financial institution records and whether statutorily required investment information was presented timely to the Board. Also, we determined whether any investment income was properly allocated to the funds that generated the investment income.
- Evaluated University investment policies and examined University investment records to determine whether investment maturities for the University's current operating funds were reasonable.
- Examined University student fee schedules to determine whether the University had the authority for assessing such fees, the University separately accounted for the fees, and the fees did not exceed the limits established in Section 1009.24, Florida Statutes, and Board of Governors Regulations 7.001 and 7.003.
- Examined University records for distance learning courses to determine whether distance learning fees, totaling $3.6 million for the audit period, were assessed, collected, and separately accounted for in accordance with Section 1009.24(17), Florida Statutes.
- From the population of 32 decentralized cash collection locations, selected 2 locations with collections during the audit period and examined University records supporting collections totaling $385,680 to determine the effectiveness of University collection procedures.
- From the population of compensation payments totaling $135.7 million made to 5,625 employees during the audit period, selected 30 payroll transactions totaling $111,400 and examined the related payroll and personnel records to determine the accuracy of the rate of pay, the validity of employment contracts, whether the employees met the required qualifications, whether performance evaluations were completed, the accuracy of leave records, and whether supervisory personnel reviewed and approved employee reports of time worked.
- Examined severance pay provisions in 16 employee contracts to determine whether the provisions complied with Section 215.425(4)(a), Florida Statutes. Additionally, for the

2 employees who received severance pay totaling $86,553 during the audit period, we examined University records to determine whether the severance payments complied with State law and University policies.

- Examined University records to determine whether compensation paid to the President did not exceed the limits established in Section 1012.975(3), Florida Statutes.
- Examined University records to determine whether selected expenses were reasonable; correctly recorded; adequately documented; for a valid University purpose; properly authorized and approved; in compliance with applicable laws, rules, contract terms, and University policies; and whether applicable vendors were properly selected. Specifically, from the population of expenses totaling $191.7 million for the audit period, we examined University records supporting:
  - 30 selected payments for general expenses totaling $3.8 million.
  - 30 selected payments for contractual services totaling $2.6 million.
  - 30 selected payments from restricted sources totaling $2.2 million.
  - 10 selected payments for competitive procurements totaling $2.3 million.
- Reviewed University policies and procedures related to identifying potential conflicts of interest. We also reviewed Department of State, Division of Corporations, records; statements of financial interests; and University records for the President, Trustees, and 22 University employees to identify any potential relationships that represented a conflict of interest with vendors used by the University.
- Evaluated University procedures to ensure compliance with the Florida Small Business Development Center Network grant provisions for reporting grant activities during the audit period.
- 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

ADMINISTRATION & FINANCE
Office of the Vice President

UNF UNIVERSITY of NORTH FLORIDA.

October 14, 2020

Ms. Sherrill F. Norman
Auditor General
State of Florida
111 West Madison Street
Claude Pepper Building, Suite G-74
Tallahassee, FL 32399-1450

Dear Ms. Norman:

In connection with the University of North Florida Operational Audit please find the enclosed University response to the Preliminary and Tentative audit findings dated September 16, 2020.

Should you have any questions or need additional information, please do not hesitate to contact me.

Sincerely,

Scott Bennett

Scott Bennett
Interim Vice President, Administration & Finance

Enclosure

1 UNF Drive, Jacksonville, Florida 32224-7699
Tel: (904) 620.2002 Fax: (904) 620.2010
Equal Opportunity/Equal Access/Affirmative Action Institution

Responses to Florida Auditor General's Preliminary Findings dated September 16, 2020

Finding No. 1: Severance Payments

State law provides that an employee may receive severance pay that is not provided for in a contract or employment agreement if the severance pay represents the settlement of an employment dispute and the amount does not exceed 6 weeks of compensation. State law defines severance pay as salary, benefits, or perquisites for employment services yet to be rendered that are provided to an employee who has recently been or is about to be terminated.

Recommendation: The University should continue efforts to ensure the University policies and procedures limit severance pay consistent with State law.

University Response:

Revisions are currently in-progress for the University Policy 4.0280P Separation from Employment, eliminating the practice of providing payments in lieu of a lengthy notice period, limiting severance pay consistent with State law.

Finding No. 2: Information Technology User Access Privileges – Sensitive Personal Information

The Legislature has recognized in State law 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 to help prevent employees from accessing sensitive personal information inconsistent with their duties.

Recommendation: To ensure that sensitive personal information maintained by the University is properly safeguarded, the University should:

- Complete efforts to evaluate employee access to the document imaging system and establish procedures to periodically conduct future evaluations to ensure that such access is necessary based on employee job duties.
- Document the viable public purpose for maintaining that information for prospective students who do not enroll in the University, establish a reasonable time frame for maintaining the information, and delete the information when the time frame expires.
- Upgrade the University IT system to include a mechanism to differentiate access privileges to former, prospective, and current student information. Additionally, if an employee only requires occasional access to the sensitive personal information, the access should be granted only for the time needed.

University Response:
The University agrees and recognizes the importance to protect sensitive personal information and restrict access to only those with a demonstrated business need. We will continue to evaluate our practices and procedures and determine how best to further safeguard this information. Specifically:

- Procedures are being updated to include more periodic reviews of those with access to the imaging system to ensure continued need in accordance with employee job duties.
- The purging of prospective student information after an established period of time for those individuals who do not enroll in the University.
- We will include in our procedures the practice of granting access for a time limited period, if appropriate. It should be noted that this is infrequent, as access is only granted if needed for an employee to perform their established job duties. As indicated in previous audits, the current ERP system does not allow for the differentiation of student records based on the categories of former, prospective, or current students.