FIU | FLORIDA INTERNATIONAL UNIVERSITY

Office of Internal Audit

Audit of the Robert Stempel College of Public Health and Social Work

Report No. 17/18-06

January 16, 2018

FLORIDA INTERNATIONAL UNIVERSITY

OFFICE OF INTERNAL AUDIT

MEMORANDUM

DATE: January 16, 2018

TO: Tomàs R. Guilarte, Dean, Robert Stempel College of Public Health & Social Work

FROM: Allen Vann, Chief Audit Executive

SUBJECT: **Audit of the Robert Stempel College of Public Health & Social Work Report No. 17/18-06**

We have completed an audit of the Robert Stempel College of Public Health and Social Work, which included internal controls relating to revenues, payroll administration, procurement of goods and services, travel and property accounting. We also evaluated lab safety and information security controls.

The College's interdisciplinary structure combines its departments of public health in partnership with the disciplines of dietetics and nutrition, social work and disaster preparedness. Total enrollment for Fall 2016 was 571 undergraduate and 536 graduate students. For fiscal year 2017, the College spent $13.7 million from Educational & General (E&G) funding and $232,000 from auxiliary funding sources.

Our audit disclosed that the College's established controls relating to revenues and expenditures were good and adequate processes were in place to monitor its fiscal activities. We found some opportunities where internal controls could be strengthened, particularly pertaining to: the payroll approval process, asset management and information security controls over research data. The audit resulted in 12 recommendations, which management agreed to implement.

We would like to take this opportunity to express our appreciation to you and your staff for the cooperation and courtesies extended to us during the audit.

Attachment

C: FIU Board of Trustees
Mark B. Rosenberg, University President
Kenneth G. Furton, Provost and Chief Operating Officer
Kenneth A. Jessell, Chief Financial Officer and Senior Vice President
Javier I. Marques, Chief of Staff, Office of the President
Elizabeth Bejar, Vice President for Academic Affairs
Robert Grillo, Vice President of Information Technology and CIO
Barbara Manzano, Assistant Vice Provost Planning & Finance
Paola Moreno, Executive Director Operations, College of Public Health & Social Work

TABLE OF CONTENTS

OBJECTIVE, SCOPE AND METHODLOGY

Pursuant to our approved annual plan, we have completed an audit of the Robert Stempel College of Public Health and Social Work (Stempel College or College). The primary objectives of our audit were to determine if established controls and procedures relating to revenues, payroll administration, procurement of goods and services, travel and property accounting were: (1) adequate and effective; (2) being adhered to; and (3) in accordance with University policies and procedures, applicable laws, rules and regulations. We also evaluated lab safety and information security controls over sensitive or confidential data.

Our audit included the College's financial transactions for the fiscal year 2016-2017. The audit was conducted in accordance with *the International Standards for the Professional Practice of Internal Auditing*, and included test of the accounting records and such other auditing procedures, as we considered necessary under the circumstances. Sample sizes and transactions selected for testing were determined on a judgmental basis. Audit fieldwork was conducted from May to October 2017.

During the audit, we:

- Reviewed University policies and procedures and applicable Florida Statutes and regulations;
- Observed current practices and processing techniques at the College;
- Interviewed responsible personnel; and
- Tested selected transactions.

As part of our audit, we reviewed internal and external audit reports issued during the last three years to determine whether there were prior recommendations related to the scope and objectives of this audit and whether management had effectively addressed prior audit concerns. There were no prior audit recommendations related to the scope and objectives of this audit that required follow-up.

BACKGROUND

The Robert Stempel College of Public Health & Social Work is one of eleven academic colleges at FIU and is located in Academic Health Center 5 at the Modesto Madique Campus.

In January 2016, the University appointed a new Dean to the College whose mission and vision is to advance and integrate health and social welfare by seeking excellence in education. Its research and services benefit diverse communities in South Florida by sharing and applying knowledge, wisdom and ethical decision making in public health and social welfare.

Stempel College's interdisciplinary structure combines its departments of public health in partnership with the disciplines of dietetics and nutrition, social work and disaster preparedness.

It includes the:

- School of Public Health;
    - Biostatistics
    - Environmental Health Sciences
    - Epidemiology
    - Health Policy & Management
    - Health Promotion & Disease Prevention
- Department of Dietetics & Nutrition;
- School of Social Work; and
- Academy for International Disaster Preparedness.

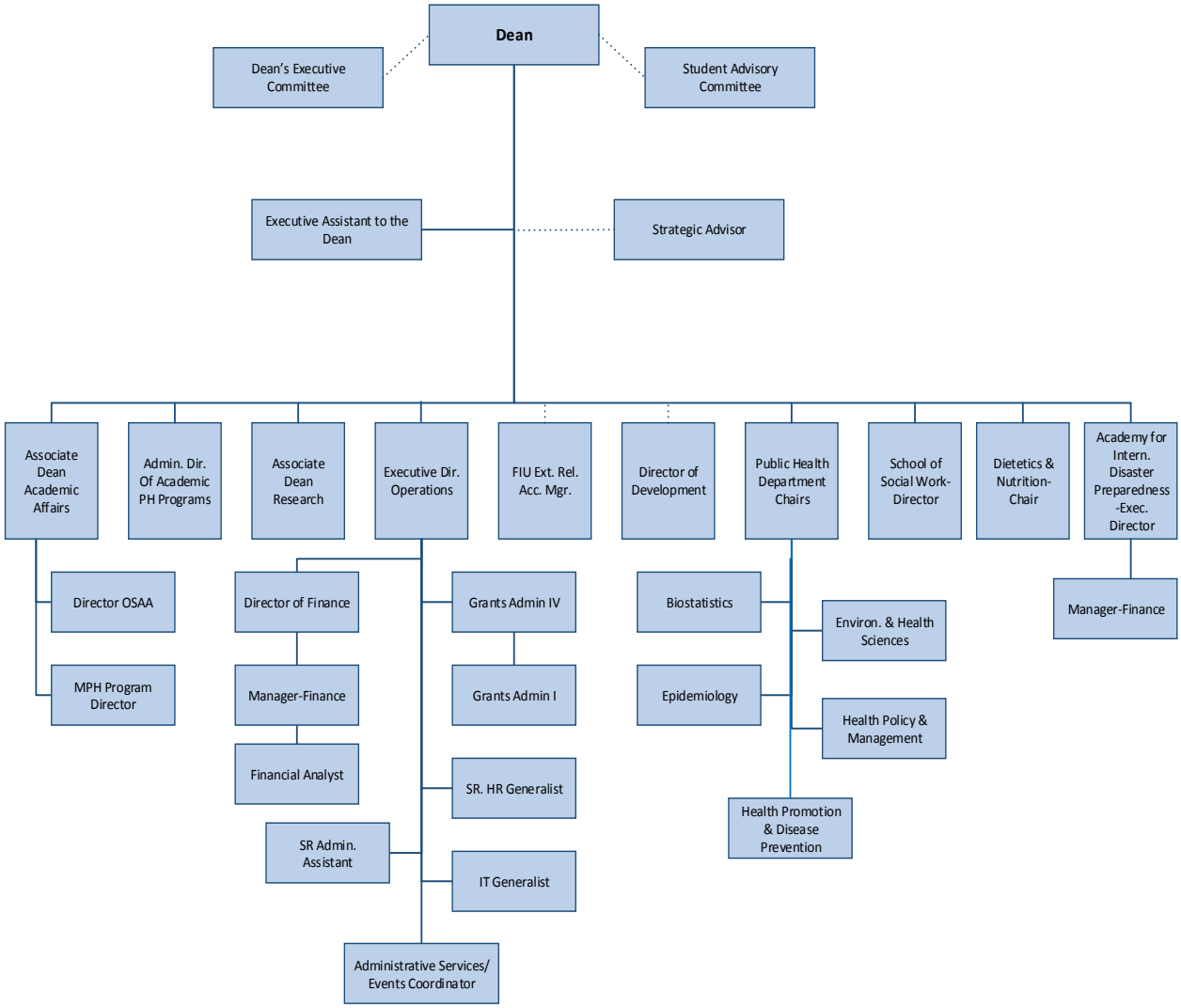
Stempel College offers undergraduate degrees, graduate degrees, and/or certificates for nine academic programs. The College's total enrollment for Fall 2016 was 571 undergraduate and 536 graduate students.

Additionally, the College has several closely affiliated and emerging research centers. These include the FIU-Banyan Research Institute on Dissemination, Grants & Evaluation (FIU-BRIDGE) and the Center for Research on U.S. Latino HIV/AIDS and Drug Abuse (CRUSADA). In September 2017, FIU-BRIDGE was awarded a $13.1 million grant from the National Institute on Minority Health and Health Disparities to create the first Health Disparities Research Center at a Minority Institution in Florida (FIU-RCMI). Likewise,

nearly $6.9 million was recently awarded to launch the Center for Latino Health Research Opportunities (CLaRO). CLaRO is part of CRUSADA and is a partnership with the University of Miami's School of Nursing and Health Studies. These grants will address substance use problems, psychological trauma, mental health problems and HIV/AIDS among Latino communities in Miami-Dade County.

Personnel

As of May 2017, the College had 97 faculty, 16 adjuncts, 29 administrative personnel and 20 staff members. The organization chart is shown below.



Financial Information

For the fiscal year 2016-17, $13.7 million was spent from Educational & General (E&G) funding and expenditures from auxiliary funding sources totaled $232,000, as detailed in the following table.

E&G and Auxiliary Expenditures Fiscal Year 2016-2017			
Category	**E&G**	**Auxiliary**	**Total**
Salaries and Benefits:			
Faculty	$ 7,127,015	$ 29,691	$ 7,156,706
Admin	1,334,836	22,274	1,357,110
Staff	511,484	-	511,484
Adjunct Faculty & Graduate Assistants	845,738	33,982	879,720
Student Assistants & Work Study	15,464	660	16,124
Temporary Employees	79,229	5,319	84,549
Fringe Benefits	3,005,907	6,368	3,012,274
Other Earnings/Misc. Payroll	78,201	1,100	79,301
Total Salaries and Benefits	**$ 12,997,874**	**$ 99,394**	**$ 13,097,268**
Other Operating Expenses:			
Materials, Supplies & Postage	$ 527,152	$ 104,148	$ 631,300
Travel	75,733	6,333	82,066
Telecommunications	59,728	1,940	61,668
Xerox Copies (Toshiba Lease/Usage)	15,889	-	15,889
Cellphones	2,950	-	2,950
Shared Service Fees	-	15,092	15,092
Bad Debt Expense	-	432	432
Miscellaneous	-	4,421	4,421
Total Other Operating Expenses	**$ 681,452**	**$ 132,366**	**$ 813,818**
Total Expenditures	**$ 13,679,326**	**$ 231,760**	**$ 13,911,086**

FINDINGS AND RECOMMENDATIONS

Our audit disclosed that the College's established controls relating to revenues and expenditures were mostly good. Nevertheless, there were areas where internal controls need strengthening, particularly pertaining to: payroll and personnel administration, expenditure controls and asset management. In addition, we observed areas where there are opportunities to improve IT controls.

Our overall evaluation of internal controls is summarized in the table below.

INTERNAL CONTROLS RATING			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls		**X**	
Policy & Procedures Compliance	**X**		
Effect	**X**		
Information Risk		**X**	
External Risk		**X**	
INTERNAL CONTROLS LEGEND			
CRITERIA	**SATISFACTORY**	**FAIR**	**INADEQUATE**
Process Controls	**Effective**	**Opportunities exist to improve effectiveness**	**Do not effectively safeguard assets**
Policy & Procedures Compliance	**Non-compliance issues are minor**	**Non-compliance Issues may be systemic**	**Non-compliance issues are pervasive, significant, or have severe consequences**
Effect	**Not likely to impact operations or program outcomes**	**Impact on outcomes contained**	**Negative impact on outcomes**
Information Risk	**Information systems are reliable**	**Data systems are mostly accurate but can be improved**	**Systems produce incomplete or inaccurate data which may cause inappropriate financial and operational decisions**
External Risk	**None or low**	**Medium**	**High**

The areas of our observations during the audit are detailed below.

1. Financial Management

During the audit, we observed that the College has adequate processes in place to monitor its fiscal activities, including budget management, analysis of revenues and expenses, forecasting and planning of expenditures, reconciliation of accounts and monitoring of spending. For example, a Financial Overview Report is provided to the chair of each department on a monthly basis. The report informs managers on year-to-date spending activity and available balances for their respective department and is utilized to help keep track of budget variances. In addition, the College developed an approval matrix for appropriate level review and approval of expenses at the Dean's office level.

Although the College has been operating in a fiscally responsible manner, we noted they did not follow standard processes among their departments. For example, the process to hire new faculty and bring them on-board is handled differently by each department. Management acknowledged a need for developing a comprehensive manual to standardize its practices across its operational units.

Written operational procedures serve as a reference source for employees, provide direction to new personnel, clarify responsibilities and help to assure consistent application of management's expectations. They also prove valuable when employee substitution or turnover occurs.

Recommendation

The College of Public Health & Social Work should:	
1.1	Develop an operations manual to standardize processes and govern the operations of the College.

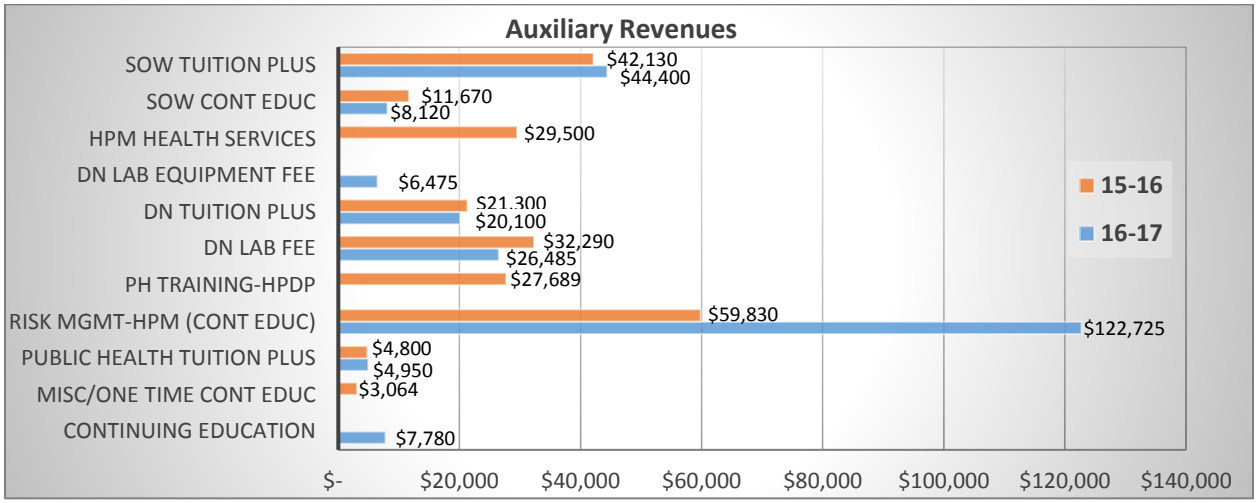
Management Response/Action Plan:

The college will develop an operations manual in order to standardize operational processes and serve as a uniform guide to the college and its departments. Initial communication and periodic reminders of the operations manual will be disseminated to college employees.

Implementation Date: July 31, 2018

2. Revenue Controls

The main sources of auxiliary revenue are received from continuing education courses, tuition-plus courses, lab fees and material and supply fees. For fiscal year 2016-17, auxiliary revenues totaled $241,533. The graph below reflects the source and amount of revenue earned by the College for the past two fiscal years.



Its largest auxiliary, the Risk Management in the Health Sector program and Healthcare Advancement Conference, earned $122,725 which represented approximately 51% of total auxiliary revenue earned during the audit period. The Certificate in Risk Management in the Health Sector is a six-month comprehensive learning experience offered in Spanish to healthcare professionals in Latin America. The program is taught by faculty in the College's Health Policy and Management department and consists of five hybrid courses with two onsite learning components held at FIU in Miami, Florida and Universidad ESAN in Lima, Peru. Initially when the program began in 2014, the College entered into an agreement with Universidad ESAN to offer the certificate program to graduate students enrolled at ESAN. In academic year 2016-17, participation became open to non-ESAN graduate students as well, and the program's revenues increased by $37,115 or 62% over the prior fiscal year. Also, the Healthcare Advancement Conference generated additional revenue of $25,780.

During the audit, we tested 15 revenue transactions totaling $52,531. Our test disclosed that all revenues were appropriate, properly assessed, collected and recorded in the correct account. As part of the testing, we also determined that revenue received from Universidad ESAN was accurate and in accordance with the contractual agreement for the program. No exceptions were noted in this area.

3. Payroll and Personnel Administration

Salaries and fringe benefits were approximately $13.4 million, representing 85% of the College's total expenditures during the audit period. We reviewed the processes for payroll approval, employee background checks and overload compensation.

a) Payroll Approval

The University's payroll guidelines require managers/proxies to have first-hand knowledge of the employee's work and/or leave hours or obtain written confirmation from the employee's supervisor of the hours being reported prior to approving the payroll.

We reviewed time and attendance records for the entire 2016-17 fiscal year, which consisted of 9,083 transactions. Our review revealed that payroll was approved by the employee's direct supervisor 34% of the time and a designated proxy other than the supervisor 56% of the time. We determined that a process was established for the designated proxies to document and maintain support for their approval of time and leave. However, the remaining 10% was not approved by either the supervisor or the designated proxy; therefore, they were automatically approved by the University's Payroll Department without having first-hand knowledge of the employees' time and leave hours taken.

In addition, we selected 47 employees whose employment with the College ended to ensure they were timely removed from the payroll and did not receive unearned salary. Our review disclosed that 94% (44 out of 47) of the employees tested were timely removed without any additional pay received. Three employees received pay after their termination dates, which resulted from late submission of previous time worked by the former employee or their supervisor. However, we determined that the pay was valid.

Per the University's payroll guidelines, managers must ensure that all employees have submitted their time and/or leave entries and managers must sign-off by Monday of the pay week. Thus, timely submission and approval of hours are required to ensure employees are accurately and timely compensated for hours worked.

Absence of an adequate payroll approval process could leave the University vulnerable to paying employees for time not worked or lead to inaccurate time and leave records, which can be costly in the long term.

b) Employee Background Checks

According to FIU Policy No. 1710.257, *Background Check Requirements,* background investigations will be conducted based on the job-related requirements and consistent with business necessity. The policy applies to new hires, individuals rehired after a break in service, and current administrative or staff employees promoted or transferred into a position requiring more extensive background checks. More in-depth criminal history checks including fingerprinting, through the Florida Department of Law Enforcement, are required for positions such as those handling or managing cash transactions or information technology.

During our testing, we selected five new-hires and six employees who were in financial services and/or information technology related positions. We observed that criminal background checks were not on file for two of the eleven employees selected. Per discussion with Human Resources (HR), one of the employees had been in their position several years prior to the implementation of the policy, thus, was "grandfathered in." The other employee's background check was performed in 2010 when she was hired at the University; therefore, when she transferred to the College in 2014, another background check was not necessary.

c) Overload Compensation

FIU Policy No. 1710.110, *Dual Employment and Compensation*, states that "All employees may be approved for secondary employment, which constitutes dual employment provided such employment does not interfere with the regular work of the employee, does not result in any conflict of interest between the two activities, and is determined as being in the best interest of the University…approval for extra compensation must be secured from the employee's supervisor, prior to contracting for services, including instructional and non-instructional activities."

The College had 17 faculty that received extra state compensation in the fall 2016 and/or spring 2017 semesters. We selected six employees and reviewed the eRequest for Additional Compensation (eRAC) forms and associated contracts, totaling $19,125. Our review disclosed that the secondary assignments did not result in any conflict of interest and were primarily for teaching courses outside of the employee's normal working schedule. In addition, four of the six contracts reviewed were timey submitted and approved prior to the commencement of the additional workload, but we noted two contracts that were not approved until 8 and 83 days after the work began.

Delays in approval of additional compensation or overload assignments may have an adverse impact on the College's budget and expenditure controls.

Recommendations

The College of Public Health & Social Work should:	
2.1	Ensure timely submission and approval of hours by managers/supervisors who have direct knowledge of the employees' time and/or leave.
2.2	Ensure that eRAC forms and contracts are approved prior to the commencement of secondary employment.

Management Response/Action Plan:

2.1 The Dean will communicate, in writing, the importance of timely submission and approval of work and/or leave hours reported biweekly. The college's HR liaison will continue to send biweekly e-mail reminders to the managers/supervisors regarding the current pay period's timely submission and approval of hours.

The college will implement the University's recommended e-leave process for administrative & staff employees for leave requests. Training will be facilitated for such implementation.

Implementation Date: February 28, 2018

2.2 The Dean will request, in writing, that the departments submit the eRequest for Additional Compensation (eRAC) forms with sufficient time in advance so that that the overload payment contracts are approved "before" the secondary assignment start date.

Implementation Date: February 28, 2018

4. Expenditure Controls

We selected 60 transactions totaling $82,508, which included foundation and grant expenses. They were related to travel, use of student fees, credit card controls and procurement of goods and services. Except for some of the observations noted below our audit disclosed that the College's expenditures tested were appropriate, allowable, and in accordance with University policies and procedures, applicable laws, rules and regulations.

a) Travel Authorizations

According to Florida Statute section 112.061(3)(a), "All travel must be authorized and approved by the head of the agency, or his or her designated representative, from whose funds the traveler is paid…" In addition, FIU Policy No. 1110.060, U*niversity Travel Expense Policy,* requires travelers not to make commitments to travel or to incur travel expenses without first obtaining the appropriate approval.

We noted that the Travel Authorization (TA) for two transactions totaling $850 was not prepared and submitted for approval prior to incurring travel related expenses. Both transactions were for the purchase of airfare tickets. One ticket was purchased with the Department's credit card, while the other was purchased with the employee's personal credit card.

The payment of travel expenses using the procurement card or by the traveler is prohibited without an approved TA. The use of a travel authorization helps to ensure travel expenses are authorized and are within established budgetary limits for the department or project funds being expended.

b) Credit Card Controls

During the audit period, the College had 22 active cardholders, with 1,369 credit card transactions, representing approximately $444,000 in expenses. We reviewed credit card transaction activity to ensure proper segregation of duties existed between the cardholder and the approver. We determined that proper segregation of duties existed between the cardholder and approver, as designated approvers were not subordinates of the cardholders. We also met with three cardholders to evaluate processes in place for review and reconciliation of credit card charges. Based on our observation, we determined that an adequate process existed.

However, our review disclosed that three employees were still listed as authorized approvers for seven of the cardholders tested, although one was no longer an authorized approver, the second employee transferred to another department over four years ago, and the third person was terminated from the University. Per the Departmental Card Guidelines & Procedures Manual, "The Credit Card Solutions Team must be notified immediately by the cardholder, their approver, or by the cardholder's department whenever the cardholder retires, resigns, terminates employment, transfers to another department, or assumes different duties that do not require using the departmental card."

Upon our inquiry, the Credit Card Solutions Administrator further researched the issue and requested the College to complete the Approver/Reconciler Request Form to have the employees removed as approvers. We also noted that no transactions were approved by them during the audit period.

c) Accounting Classification

Although transactions tested were allowable, adequately supported and related to the operations of the College, we noted classification errors with seven expenditures, totaling $1,979, which were charged to the incorrect expense account. For example, a $665 dinner for PhD recruits was expensed as food products/supplies used in research or academic laboratories and a $345 payment for a publishing fee was incorrectly classified as Incidental Expenses - Out of State.

The Reference Chart for Expense Accounting Codes provided by the Controller's Office is designed to assist the end user with selecting the appropriate accounts for expense coding purposes.

d) Use of Student Fees

Board of Governors (BOG) Regulation 7.003(7) allows the University to assess student fees, such as a material and supply fee, to offset the cost of materials or supply items, which are consumed in the course of the student's instructional activities. Accordingly, proceeds should be used for the instruction of the course and directly by the students.

We reviewed the College's activity numbers for courses in which student fees are assessed for material and supplies, lab equipment and tuition-plus. Related expenditures for these accounts were approximately $102,000 during the audit period. We tested 10 transactions, totaling $12,804, and determined that student fees were properly used for intended purposes.

e) Foundation Expenses

The College's Foundation expenses totaled $419,650 for the audit period. We tested 10 transactions, totaling $13,282, and determined that expenditures were appropriate and in accordance with the Foundation's policies and procedures.

Recommendations

The College of Public Health & Social Work should:	
3.1	Ensure that travel authorizations are obtained and approved prior to employees incurring travel expenses.
3.2	Ensure to timely notify the Credit Card Solution department when employees are terminated or transfer to another department.
3.3	Ensure that expenses are properly classified and charged to the correct account.

Management Response/Action Plan:

3.1 The Director of Finance, on behalf of the Dean, will communicate, in writing, the importance of adherence to the university's travel policy to secure travel authorization prior to incurring any travel related expenses.

Implementation Date: February 28, 2018

3.2 As part of its employee separation process, the college will include an additional document, completed and signed by the supervisor and attached to the Separation of Employment/Transfer Clearance form, in order to notify the Credit Card Solution department of any employee terminated or transferred to another department who no longer is an approver and/or reconciler, or cardholder.

Implementation Date: Immediately

3.3 The college will make every effort to classify all expenses in accordance to the expense accounting codes and select the most appropriate even in those instances where the list of expense codes is limited due to the activity or project funding the transaction. The Director of Finance will communicate, in writing, to all staff initiating expense transactions the importance of properly selecting the applicable expense code.

Implementation Date: February 28, 2018

5. Asset Management

As of September 2017, the College had 86 capital assets with associated cost of approximately $1.2 million. The capital asset inventory as recorded in the University's asset management system was up-to-date and we confirmed with the Assistant Controller for Asset Management that no missing property was observed during the College's annual physical inventory.

In addition to managing capital assets, departments should evaluate and catalogue attractive property. The University's Property Control Manual defines attractive property as items costing less than the threshold amount of $5,000, but which are particularly vulnerable to theft and misuse. Examples include laptops, iPads or video recorders. Departments have discretion in determining the "attractiveness" in the context of their environment, but factors to consider include the security of the property location, the size and portability of the item, and its potential resale value if stolen. These items should be marked as University property, as stated in the manual.

Per discussions with the College's Information Technology Administrator, he uses an internal database to maintain a list of attractive property for the College. We were informed that recent changes within the College now requires departments to send IT related purchases to the IT Administrator to be tagged and included in the database prior to being sent to the department. As such, we obtained a copy of the Attractive Inventory List and acknowledged that he was in the process of updating it; however, we noted controls around tracking attractive property can be further improved.

During the audit, we visited the FIU-Borinquen Research Clinic, an off-campus clinic for research studies performed by faculty in the Dietetics and Nutrition department. We determined that none of the devices at the clinic, which included six laptops and four desktops, were being tracked by the College, nor were they tagged as University property. We also noted that the Attractive Inventory List did not contain information such as MAC addresses or computer host names.

FIU Policy No. 1910.005, *Responsibilities for FIU Network and/or Systems Administrators*, states, "The Network/System Administrator shall maintain and make readily available to the Division of IT all documentation of any and all devices within their unit that will attach to the University's network." Among other things, the policy says that the report must include information such as the following:

- MAC address of all network interface cards within their unit, and as appropriate any permanent Layer 3 network address.
- Computer's host name(s) and primary user's information.
- Physical location of the equipment.
- System's primary functions (e.g. web services, file server, mail server, personal computer, etc.).

In addition, according to FIU Policy No. 1670.030, *Inventory of Hardware and Software Containing Electronic Protected Health Information*, all Electronically Protected Health

Information (EPHI) accessible devices shall be accounted for and maintained in a master inventory list. Due to the type of sensitive data stored on the devices at the Clinic, it is imperative for the College to keep track of them. A comprehensive list of high-risk devices allows the University to ensure only authorized individuals have access to EPHI and that proper safeguards are in place.

Recommendations

The College of Public Health & Social Work should:	
4.1	Track all attractive/sensitive property and ensure that they are included on its Attractive Inventory list and marked as University property.
4.2	Update its Attractive Inventory list to include information required in the University Policy, such as MAC addresses and computer host name.

Management Response/Action Plan:

4.1 The college will continue to affix University property tags and include in its inventory management software (i.e. WASP) all college IT accountable and attractive/sensitive property, including those located off-campus. The Dean will communicate, in writing, a memorandum reminding employees that all IT equipment set-up is centralized through the College IT Generalist.

Implementation Date: April 2, 2018

4.2 The college's IT department will include MAC address and host names in its inventory management software.

Implementation Date: April 2, 2018

6. Lab Safety

The College has ten research labs in-house that is assigned to eleven Principle Investigators. We reviewed the laboratory inspection reports from the department of Environmental Health & Safety (EH&S) and noted that all labs were inspected within the past year. We also noted that no safety concerns were cited for seven of the ten labs reviewed.

Two of the labs, which were Biosafety Level II labs (i.e., work with infectious materials capable of causing disease, such as human cell lines or blood), received violations for things such as biohazard signs not posted on equipment where cells are handled/stored or the appropriate vaccination records not readily available for review. However, we noted that corrected actions were taken for all safety concerns and there were no outstanding issues related to lab safety.

7. Information Security Controls over Research Data

To determine if the College has controls in place to protect sensitive or confidential data, we visited the FIU-Borinquen Research Clinic, located off-campus. They have six laptops and four desktops that are used to collect sensitive data such as name, address, social security number, date of birth, phone number and blood test result.

We examined all ten endpoint devices and noted the following conditions.

a) Malicious Code Protection

Malware is defined as software that is intended to damage or disable computers and computer systems. If undetected, malware can be used to disrupt computer operations, gather sensitive information or gain unauthorized access to the Clinic's information systems. According to FIU Procedure No. 1930.020c, *IT Security Procedure: System and Application Management*, all FIU owned endpoint devices that connect to FIU's network must have anti-virus software running within 24 hours of their release.

We compared system event log files to the anti-virus logs start date and found two endpoint devices had the anti-virus installed 6 and 11 days, respectively after they started being actively used. Whereas, the other eight devices had the anti-virus installed within two days or less. There is an increased risk that the two-endpoint devices running on the network without antivirus are infected with malware.

In addition, another effective means to mitigate the risk of malicious code infection would be to set endpoint devices to perform real-time scans of all electronic files received from external sources (such as the web, email, and USB) as they are downloaded or opened. This will help to ensure the malicious code is stopped prior to affecting the device. Upon our examination, we found that one endpoint device had McAfee OnAccessScan disabled and two (using the vendor based security analysis tool) were missing 24 Microsoft Office security updates, which increase the risk of malware on the devices.

According to the procedure, the Division of IT will control the distribution of anti-virus definition files and operating system updates. In order to accomplish this, the Division of IT's Network Systems Security Engineering (NSSE) department needs to centrally manage the College's endpoint devices. However, the NSSE department only manages two of the ten endpoint devices examined. The effectiveness of antivirus controls is reduced if definition files are not updated in a timely manner and unpatched vulnerabilities allow malicious code entry points into the network.

b) Data Encryption

The purpose of hard drive encryption is to protect the data from unauthorized access in the event the device is lost or stolen. We requested that the NSSE department confirm whether the Clinic's endpoint devices were encrypted. The NSSE department responded that two of the ten devices were encrypted; however, they were unable to determine if the remaining eight devices were, since they were not managed by the Division of IT. Upon our examination, we determined that the remaining devices hard drives were not encrypted.

According to the Clinic's Research Coordinator, they utilized encrypted portable drives to share EPHI data amongst themselves. She stated that in the event the drives become corrupted, the encryption keys information is stored away in a locked file cabinet at the Clinic, on her laptop, and in an encrypted external hard drive. Sharing portable drives entails that passwords are shared with other individuals. Per FIU Procedure No. 1930.020, *Information Technology Security*, passwords shall not be shared with any other person.

The lack of encrypted devices along with the sharing of passwords increases the risk of unauthorized access to sensitive or confidential data.

c) Risk Assessment

Risk Assessments provide critical information to support risk-based decisions that take into account the business relevance of risk factors, such as threat types, frequency and magnitude of loss. The Division of IT recently conducted a Security Assessment based on Research Contracts' Data Use Agreements. However, according to the Division of IT's Information Security Office, the completed risk assessment did not include the Clinic or HIPAA related data. According to the HIPAA Security Rule §164.308(a)(1), a through risk assessment is required and must identify the potential risks and vulnerabilities to the confidentiality, integrity, and availability to EPHI data. By performing a formal risk assessment, the College will have the ability to identify and mitigate high-risk areas.

In addition, according to University Policy No. 1910.005, *Responsibilities for FIU Network and/or System Administrators*, departments' IT administrators should send a quarterly report to the Division of IT of any systems implementation or changes to the IT environment. The College's IT administrator stated that he does not send a report to the Division of IT.

d) Uniquely Identify Users

According to FIU Policy No. 1930.020a, *Data Stewardship*, all highly sensitive data must be accessed by way of a unique name for identifying and tracking user identity. By assigning a unique identification (ID) to each user account ensures that each individual is accountable for their actions. During our testing, we found that nine of the ten endpoint devices contained at least one local non-uniquely named user account with administrative privileges.

Our review also disclosed that the local administrator passwords were shared among the staff on eight of the devices tested, although FIU Procedure No. 1930.020, *Information Technology Security*, requires passwords to be not shared with any other person. Using a vendor based security analysis tool, we also found that all ten devices examined had the local administrator user accounts with non-expiring passwords. A brute-force attack that exploits a weak or nonexistent password is one method that can be used by a malicious user to compromise an endpoint device. The Division of IT's Group Policy settings specify password parameters that must be reset after a specific period of time. In addition, generic accounts and password sharing reduce the information systems' ability to track individual user actions; thereby reducing the effectiveness of identification and authentication controls.

Separately, we found that two non-IT personnel (Research Coordinator and Research Nurse) had administrator privileges to their endpoint devices. Local administrator accounts have the ability to circumvent university endpoint security controls at the device level.

Recommendations

The College of Public Health & Social Work should:	
5.1	Work with the Division of IT's Network Systems Security Engineering to ensure that endpoint devices are centrally managed and not infected by malicious code. Also, ensure that security updates are timely installed.
5.2	Work with the Division of IT to conduct a formal risk assessment and send a quarterly report to the Division of IT of any systems implementation or changes to the IT environment.
5.3	Review and disable generically named administrator accounts, discontinue password sharing and comply with the University's password parameter settings.
5.4	Review and disable administrative privileges from the two non-IT user accounts.

Management Response/Action Plan:

5.1 The college will reassess IT equipment, both on-site and off-site, to ensure devices are centrally managed, not infected by malicious code and conduct timely installation of security updates. Off-site clinic IT equipment will be re-imaged via SCCM (System Center Configuration Manager) and added to AD domain, thereby automatically ensuring security updates and encryption.

Implementation Date: July 31, 2018

5.2 The college's IT Generalist will submit a formal request to the Division of IT (DoIT) to perform and complete a risk assessment by July 2018. After such assessment, The college's IT Generalist will provide quarterly reports to DoIT of any systems implementation or changes to the IT environment.

Implementation Date: July 31, 2018

5.3 The Dean will communicate, in writing, to all employees reminding them of university policy for proper credential use. University password parameter settings and local admin accounts will be resolved once the off-site clinic devices are re-imaged and joined to AD domain.

Implementation Date: April 2, 2018

5.4 The college's IT Generalist will review and disable administrative privileges from the two non-IT user accounts.

Implementation Date: April 2, 2018