

STATE OF FLORIDA AUDITOR GENERAL

Operational Audit

Report No. 2018-106
February 2018

NORTH FLORIDA COMMUNITY COLLEGE



Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period January 2016 through December 2016, John Grosskopf served as President of North Florida Community College and the following individuals served as Members of the Board of Trustees:

	<u>County</u>
Michael R. Williams, Chair	Madison
Ricky N. Lyons, Vice Chair	Lafayette
Ann Sharon Benoit	Madison
J. Travis Coker	Taylor
Sandra K. Haas	Suwannee
David Howell	Hamilton
William D. Washington	Madison
Alton Williams, Jr.	Suwannee
Lloyd Gary Wright	Jefferson

The team leader was Tiffany R. Wilson, CPA, and the supervisor was Glenda K. Hart, 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

NORTH FLORIDA COMMUNITY COLLEGE

SUMMARY

This operational report of North Florida Community College (College) focused on selected College processes and administrative activities and included a follow-up on findings noted in our report No. 2015-021. Our operational audit disclosed the following:

Finding 1: Some unnecessary information technology user access privileges existed that increased the risk that unauthorized disclosure of student social security numbers may occur.

Finding 2: Policies and records supporting College property, facilities, and personal services used by the College direct-support organization could be improved.

Finding 3: The College needs to develop and implement a security awareness training program.

Finding 4: The College disaster recovery plan did not include all necessary elements to ensure that the College continued critical operations in the event of a disaster and the plan had not been tested.

BACKGROUND

North Florida Community College (College) is under the general direction and control of the Florida Department of Education, Division of Florida Colleges, and is governed by State law and State Board of Education rules. A board of trustees (Board) governs and operates the College. The Board constitutes a corporation and is composed of nine members appointed by the Governor and confirmed by the Senate. The College President serves as the Executive Officer and the Corporate Secretary of the Board, and is responsible for the operation and administration of the College.

The College has a campus in Madison. Additionally, credit and noncredit classes are offered in public schools and other locations throughout Hamilton, Jefferson, Lafayette, Madison, Suwannee, and Taylor Counties.

This operational audit focused on selected College processes and administrative activities and included a follow-up on findings noted in our report No. 2015-021. The results of our financial audit of the College for the fiscal year ended June 30, 2017, will be presented in a separate report. In addition, the Federal awards administered by the College are included within the scope of our Statewide audit of Federal awards administered by the State of Florida and the results of that audit, for the fiscal year ended June 30, 2017, will be presented in a separate report.

FINDINGS AND RECOMMENDATIONS

Finding 1: Information Technology User Access Privileges

The Legislature has recognized in State law¹ 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. Effective controls restrict employees from accessing information unnecessary for their assigned job responsibilities and provide for documented, periodic reviews of employee access privileges to help prevent personnel from accessing sensitive personal information inconsistent with their responsibilities.

The College collects and uses SSNs pursuant to State law for various purposes, such as providing SSNs to the Internal Revenue Service (IRS) for Federal tax purposes, enrollment verification, and reporting Veterans Administration beneficiaries. According to College personnel and records, the College established a unique identifier, other than the SSN, to identify students and also maintained SSNs in the College information technology (IT) system. As of July 2017, College personnel indicated that the IT system contained SSNs for an estimated 20,517 students, including 1,468 current students and 19,049 former and prospective students. However, according to College personnel, the IT system did not have a mechanism to differentiate user access privileges to current student information from access privileges to former and prospective student information. Additionally, College records did not demonstrate the public purpose served for maintaining SSNs for individuals who had not enrolled in the College.

To protect student information from unauthorized disclosure, modification, or destruction, the College implemented written IT procedures requiring applicable supervisors to approve employee access to sensitive data. In addition, the College implemented IT policies and procedures that require individuals who use College information resources or have access to information to agree not to disclose information improperly, use information improperly or unethically for personal or professional gain, or to discredit or harass someone. College personnel must also sign a user agreement before access privileges to IT resources are granted. However, the College had not established procedures to require periodic reviews of IT user access privileges to student SSNs to determine whether individuals had a demonstrated need for such access privileges.

Our examination of IT user access privileges in July 2017 disclosed 80 employees who had continuous access to current, former, and prospective student SSNs. However, although we requested, College records were not provided to demonstrate that 44 of these employees needed such access based on their employee job descriptions. For example, 8 of these employees were College instructors and Finance Department personnel who needed access to student records, but did not require access to student SSNs to perform their job duties. The other 36 employees included, for example, student support personnel, academic advisors, and a dual enrollment coordinator, who needed access to current student SSNs but College records did not demonstrate why the 36 employees needed continuous access to

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

former and prospective student SSNs. The existence of unnecessary access privileges increases the risk of unauthorized disclosure of student SSNs and the possibility that sensitive personal information may be used to commit a fraud against College students and others.

Recommendation: To ensure access to sensitive student information is properly safeguarded, the College should:

- Document the public purpose served by maintaining SSNs for individuals who do not enroll in the College. Absent such, the College should discontinue the practice of indefinitely maintaining prospective student SSNs.
- Upgrade the College IT system to include a mechanism to differentiate IT user access privileges to current student information from access privileges to former or prospective student information.
- Document periodic reviews of access privileges to student SSNs to determine whether such privileges are necessary and the timely removal of any inappropriate or unnecessary access privileges detected. If an employee only requires occasional access to student SSNs, the access should be granted only for the time needed.

Finding 2: Direct-Support Organization

To promote accountability over College property, facility, and personal services use, it is important that public records document the conditions for such use, document appropriate approval before the use occurs, and demonstrate appropriate use. Such records help document authorization for the use, demonstrate the reasonableness of the value associated with that use, and enhance government transparency.

State law² provides that a direct-support organization (DSO) is organized and operated exclusively to receive, hold, invest, and administer property and to make expenditures to, or for the benefit of, a Florida College System institution such as the College. Additionally, State law³ authorizes the College Board of Trustees (Board) to permit the use of College property, facilities, and personal services by a DSO, and to prescribe by rule any condition with which a DSO must comply for such use. The Board approved the North Florida Community College Foundation, Inc. (Foundation) as a DSO and the Foundation routinely receives and uses charitable contributions for the benefit of the College.

Board policies and procedures⁴ provide that the Foundation Director shall report to the College President; the College President will authorize and monitor Foundation use of College facilities, personnel, and property on a case-by-case basis; and the Foundation will regularly report to the Board. In addition, the Foundation's annual financial audit report; copies of Foundation Board meeting minutes; and certain written or verbal reports by the President about Foundation direct support information must be provided to the Board. However, while the Board approved the Foundation as a DSO permitting the use of College property, facilities, and personal services by the Foundation, the Board had not prescribed by rule any conditions with which the Foundation must comply in order to use College resources.

² Section 1004.70(1)(a), Florida Statutes.

³ Section 1004.70(3), Florida Statutes.

⁴ Board Policy and Procedure 3.24, College Support for the Foundation.

As part of our audit, we interviewed College personnel and requested for examination College records related to the Foundation. According to College personnel, during the period April 2015 through March 2016, the College provided the Foundation personal services relating to three full-time College employees and College costs associated with those services totaled \$177,391. Based on the employee job descriptions, the employees manage Foundation activities and resources, administer Foundation scholarship awards to College students, and provide program support to various College operations. Our examination disclosed that the Director of the Foundation and the College President approved monthly time sheets for these employees for this time period to certify that the reported hours were correct and that all overtime hours, vacation hours, and sick leave hours were accounted for. In addition, for that period, the College provided facilities and related services valued at \$12,000 as disclosed on the Federal IRS Return of Organization Exempt from Income Tax Form 990 and in the Foundation's audited financial statements. According to College personnel, this amount was based on the estimated value of rent for the office space; however, although we requested, College records were not provided to support the basis for the estimated value.

In response to our inquiries, College personnel indicated that, although the Board did not separately approve personal service use and the related value, the in-kind contribution amount provided by the College related to Foundation use of College services was specifically disclosed each year in the Foundation's audited financial statements presented to and approved by the Board. Notwithstanding this response, we found that College records associated with Foundation use of College resources could be improved by prescribing in Board-approved rule any conditions with which the Foundation must comply in order to use College resources. Such rule could prescribe, for example, conditions to:

- Restrict Foundation use of College resources to those Board-approved public purposes consistent with the mission, vision, and values of the College.
- Require Foundation management to certify that College resources will only be used for Board-approved purposes and to affirm, after use, that the resources were only used for such purposes.

College records could also be enhanced by obtaining Board approval of anticipated Foundation use of College resources and the value of such use before the use occurs and documenting when the Foundation used College resources and the purpose for and value of such use. Such records would document authorization, demonstrate the reasonableness of the value, and enhance transparency for the College resources provided for Foundation use.

Recommendation: We recommend that:

- **The Board prescribe by rule any conditions with which the Foundation must comply in order to use College property, facilities, and personal services.**
- **The College document Board consideration and approval of the Foundation's anticipated use of College resources, at least annually, before the use occurs. To enhance transparency, Board approval documentation should identify the square footage of the office space and related buildings that will be used by the Foundation and the estimated value of the College resources provided.**

Finding 3: Information Technology – Security Awareness Training Program

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

Although the College provided initial training to staff and made staff aware of the employee handbook, which contains information related to acceptable use and security of IT resources, the College had not implemented a comprehensive security awareness training program or performed ongoing training for College staff regarding security responsibilities, including password protection and usage, copyright issues, malicious software and virus threats, workstation and personal mobile device controls, and handling of sensitive and confidential information. The absence of a comprehensive security awareness training program increases the risk that the College's employees may not be aware of the importance of the information being handled and their responsibilities for maintaining the confidentiality, integrity, and availability of College data and IT resources.

Recommendation: The College should develop and implement a comprehensive security awareness training program for all users of IT resources.

Finding 4: Information Technology – Disaster Recovery Plan

Disaster recovery planning is an important element of IT controls established to manage the availability of valuable data and computer resources in the event of a disruption. The primary objective of disaster recovery planning is to provide the entity a plan for continuing critical operations in the event of a major hardware or software failure. The effectiveness of a disaster recovery plan requires key elements such as step-by-step procedures for recovery, identifying an alternative processing facility to be used in the event of a disaster, and contracting for use of the facility and testing of the plan.

The College Disaster Recovery Plan was designed to provide a written and tested plan directing the computer system recovery process in the event of an interruption in continuous service resulting from an unplanned and unexpected disaster. The plan included some key elements, such as identification of key recovery personnel and critical applications, and providing for backup of critical data sets. However, the College had not included step-by-step procedures for recovery nor had it identified alternative processing facilities, and the plan had not been tested as of September 2017. College personnel indicated that they intend to update the plan for all necessary procedures for recovery and contract for an alternative processing facility in the near future.

Without an effective, comprehensive disaster recovery plan and annual testing of the plan, there is an increased risk that the College may be unable to continue critical IT operations, or maintain availability of information systems data and resources in the event of a disruption of IT operations.

Recommendation: The College should complete an effective, comprehensive disaster recovery plan by providing step-by-step procedures for recovery and identifying and contracting with alternative processing facilities. In addition, once developed, the College should test the plan at least annually.

PRIOR AUDIT FOLLOW-UP

The College had taken corrective actions for findings included in our report No. 2015-021.

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 2017 through November 2017 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this operational audit were to:

- Evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, rules, regulations, contracts, grant agreements, and other guidelines.
- Examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, reliability of records and reports, and safeguarding of assets, and identify weaknesses in those controls.
- Determine whether management had taken corrective actions for findings included in our report No. 2015-021.
- Identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

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

As described in more detail below, for those programs, activities, and functions included within the scope of our audit, our audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the program, activity, or function; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests,

analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included transactions, as well as events and conditions, occurring during the audit period January 2016 through December 2016, and selected College actions taken prior and subsequent thereto. Unless otherwise indicated in this report, these records and transactions were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

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

In conducting our audit, we:

- Reviewed College information technology (IT) policies and procedures to determine whether the policies and procedures addressed certain important IT control functions, such as security, systems development and maintenance, and disaster recovery.
- Reviewed College procedures for maintaining and reviewing employee access to IT resources. We examined College records supporting the access privileges for the 10 employees with access to the database and finance and human resources applications during the audit period to determine the appropriateness and necessity of the access privileges based on employees' job duties and user account functions and whether the access prevented the performance of incompatible duties. We also examined administrator account access privileges granted and procedures for oversight of administrator accounts for the network, operating system, database, and application to determine whether these accounts had been appropriately assigned and managed.
- Reviewed College procedures to prohibit former employees' access to electronic data files. From the population of 31 employees who separated from College employment during the period July 2015 through December 2016, we examined the access privileges for 27 former employees to determine whether their access privileges had been timely deactivated.
- Evaluated the College's written security policies and procedures governing the classification, management, and protection of sensitive and confidential information.
- Evaluated the appropriateness of the College's comprehensive IT disaster recovery plan to determine whether it was in place and 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 developed to document the College's risk management and assessment processes and security controls intended to protect the confidentiality, integrity, and availability of data and IT resources.
- Determined whether the College had established a comprehensive IT security awareness and training program.
- Evaluated College policies and procedures for protecting student social security numbers (SSNs). Specifically, we examined College records supporting the access privileges of the 80 employees

who had access to student SSNs to determine the appropriateness and necessity of the access privileges based on the employees' assigned job responsibilities.

- Examined Board of Trustees, committee, and advisory board meeting minutes to determine whether Board approval was obtained for the 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 College records, to determine whether the College informed students and employees at orientation and on its Web site of the existence of the Florida Department of Law Enforcement sexual predator and sexual offender registry Web site and the toll-free telephone number that gives access to sexual predator and sexual offender public information as required by Section 1006.695, Florida Statutes.
- Examined College records to determine whether the College had developed and disseminated an anti-fraud policy and procedures to provide guidance to employees for communicating known or suspected fraud to appropriate individuals. Also, we examined College records to determine whether the College had implemented appropriate and sufficient procedures to comply with its anti-fraud policy.
- Examined College records to determine whether:
 - The Board had prescribed by rule the conditions with which the Foundation must comply in order to use College property, facilities, and personal services.
 - The Board documented consideration and approval of the Foundation's anticipated use of College resources.
 - The College required and maintained College records to document when the Foundation used College property and facilities, the purpose of such use, and the value of that use.
 - The College maintained records to document the College employee actual time and effort provided for the Foundation, the purpose for such services, and the value of those services.
- Examined College records to determine whether student receivables were properly authorized, adequately documented, properly recorded, and complied with Section 1010.03, Florida Statutes, and Board policies. Specifically, from the population of 724 student receivables recorded as of March 22, 2017, ranging in age from 0 to 91 days and totaling \$94,630, we examined documentation related to 30 selected student receivables totaling \$31,385 and determined whether the College's collection efforts were adequate and restrictions on student records and holds on transcripts and diplomas were appropriate and enforced for students with delinquent accounts.
- Examined College records to determine whether the College had established procedures to cancel the registration of students who did not timely pay fees and made student status and residency determinations in compliance with Section 1009.21, Florida Statutes.
- From the population of auxiliary operations generating total revenue of \$497,234 for the 2015-16 fiscal year we examined two auxiliary operations, food services and bookstore, which generated revenue totaling \$393,920 for the 2015-16 fiscal year, to determine whether the College properly monitored compliance with the contract terms for fees, insurance, and other provisions. Also, we performed analytical procedures to determine whether the College's auxiliary services were self-supporting.
- Evaluated whether the College's policies and procedures regarding textbook affordability for the 195 textbooks adopted for the 2017 Spring term were in accordance with Section 1004.085, Florida Statutes.
- From the compensation payments totaling \$3.8 million to 279 employees for the period July 1, 2016, through February 28, 2017, selected 30 payroll transactions totaling \$77,410 and

examined the related payroll and personnel records to determine the accuracy of the rate of pay and whether supervisory personnel reviewed and approved employee reports of time worked.

- Evaluated College policies and procedures for payments of accumulated annual and sick leave (terminal leave pay) to determine whether the policies and procedures promoted compliance with State law and Board policies. Specifically, from the population of 21 employees who separated from College employment during the audit period and were paid \$57,262 for terminal leave, we selected 7 employees who received terminal leave payments totaling \$46,195 and examined the supporting records to evaluate the payments for compliance with Sections 110.122 and 1012.865, Florida Statutes and Board policies.
- Examined College compensation records for employees (including the President) to determine whether the amounts paid exceeded the limits established in Sections 1012.885 and 1012.886, Florida Statutes.
- Evaluated the College's policies and procedures for obtaining personnel background screenings to determine whether individuals in positions of special trust and responsibility, such as positions with direct contact with persons under age 18, had undergone the appropriate background screenings. Specifically, we examined background screening records for the 35 employees in positions of special trust and responsibility and employed by the College during the period January 1, 2016, through February 28, 2017.
- Examined College expenditure documentation to determine whether the expenditures were reasonable, correctly recorded, and adequately documented; for a valid College purpose; properly authorized and approved; and in compliance with applicable laws, contract terms, and Board policies; and applicable vendors were properly selected and carried adequate insurance.
 - From the population of general expenditures totaling \$2.4 million for the period July 1, 2016, through February 28, 2017, we examined documentation relating to 30 selected payments for general expenditures totaling \$73,989.
 - From the population of contractual services expenditures totaling \$1.1 million for the period January 1, 2016, through December 31, 2016, we examined documentation related to 18 payments for contractual or professional services totaling \$224,518 related to 6 contracts.
- From the population of purchasing card (P-card) transactions totaling \$45,871 during the audit period, examined College records supporting 17 selected P-card transactions totaling \$20,146 to determine whether the P-card program was administered in accordance with College policies and procedures and transactions were not of a personal nature.
- Examined P-card records for the one cardholder who separated from College employment during the audit period to determine whether the P-card was timely canceled upon the cardholder's employment separation.
- From the population of 164 payments totaling \$82,993 during the audit period to employees for other than travel and compensation, examined 25 selected payments totaling \$8,674 to determine whether such payments were reasonable, adequately supported, for valid College purposes and whether such payments were related to employees doing business with the College, contrary to Section 112.313, Florida Statutes.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe the matters requiring corrective actions. Management's response is included in this report under the heading **MANAGEMENT'S RESPONSE**.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each College on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.



Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE



Office of the
President

January 24, 2018

Ms. Sherrill F. Norman
State of Florida Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee FL. 32399-1459

Dear Ms. Norman,

This letter is in response to our receipt of the list of preliminary and tentative findings and recommendations made to North Florida Community College as a result of the operational audit for the fiscal year ending December 31, 2016. There were four findings in this report.

Finding No. 1 – Information Technology and User Access Privileges

North Florida Community College agrees with this finding and is implementing the recommended corrections.

Finding No. 2 – Direct Support Organization

North Florida Community College agrees with this finding and is implementing the recommended corrections.

Finding No. 3 – Information Technology – Security Awareness Training Program

North Florida Community College agrees with this finding and is implementing the recommended corrections.

Finding No. 4 – Disaster Recovery Plan

North Florida Community College agrees with this finding and is implementing the recommended corrections.

Sincerely,


John Groskopf, President
North Florida Community College

325 NW Turner Davis Dr.
Madison, Fl. 32340
Telephone 850-973-1600
www.nfcc.edu

Cc: Glenda Hart, Audit Supervisor