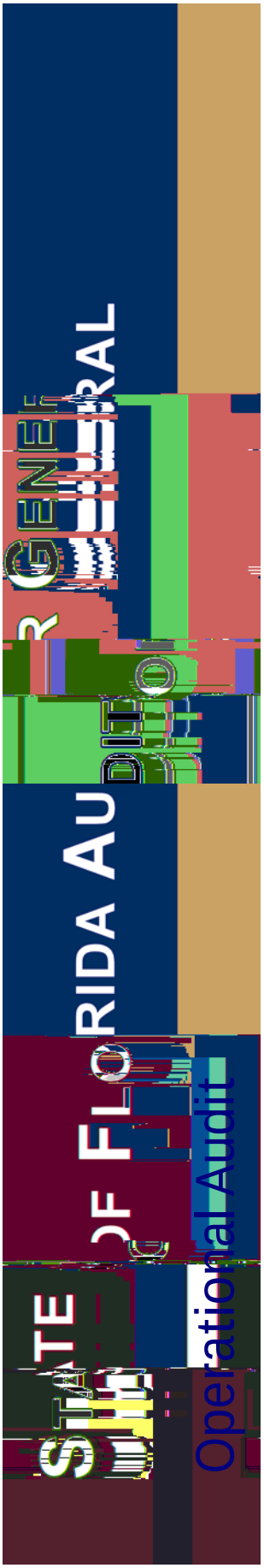


Report No. 2020-014
August 2019

UNIVERSITY OF SOUTH FLORIDA

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period January 1, 2018 through December 31, 2018, Dr. Judy L. Genshaft served as

81,9(56,7< 2) 6287+)/25,'$

SUMMARY

7KLV RSHUDWLRQDO DXGLW RI 8QLYHUVLW\ RI 6RXWK)ORULGD 8QLY... DQG DGPLQLVWUDWLYH DFWLYLWLHV... RSHUDWLRQDO DXGLW GLVFORVHG WKH IROORZLQJ

)LQGLQJ

removal may be achieved by masking the information from individuals who do not need it to perform their assigned duties.

Upgrade the University IT system to include a mechanism to differentiate current, former and prospective student information.

Finding 2: Severance Payments

State law[2] provides that a unit of government that enters into a contract or employment agreement, or renewal or renegotiation of an existing contract or employment agreement, that contains a provision for severance pay must also include a provision in the contract or employment agreement that precludes severance pay from exceeding 20 weeks of compensation and prohibits the pay in instances of misconduct. State law further provides that an employee or contractor may receive severance pay that is not provided for in a contract or employment agreement if the 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.

According to University records, 19 employees received severance payments totaling $609,810 for the 2018 calendar year. One of these employees also received severance payments totaling $134,674 during the period April 2017 through December 2017. We examined University records supporting selected payments totaling $500,428 made to 6 of the 19 employees and noted that 1 employee received an amount in excess of that established in State law. Specifically, the University

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 2018 calendar year audit period 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 University 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.

Evaluated University procedures for maintaining and reviewing employee access to IT resources. We examined access privileges over the database to critical roles within the finance and human resources applications during the audit period for 60 and 50 employees, respectively, to determine the appropriateness and necessity of the access privileges based on the employees' job duties and need to separate 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.

Evaluated University procedures that prohibit former employees' access to University IT data and resources. Specifically, we examined the access privileges for 33 of 835 former employees to determine whether their access privileges had been timely deactivated.

Evaluated University procedures for protecting sensitive personal information of students, such as student social security numbers (SSNs). Specifically, we examined University records supporting the access privileges of employees who had access to SSNs ri rioœ l

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 for the audit period to document the University risk management and assessment processes and security controls intended to protect the confidentiality, integrity, and availability of data and IT resources.

Evaluated the University data center's physical access controls, as of April 15, 2019, to determine whether vulnerabilities existed.

Examined Board of Trustees (Trustees), committee, and advisory board 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 for the audit period to determine whether the University 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.

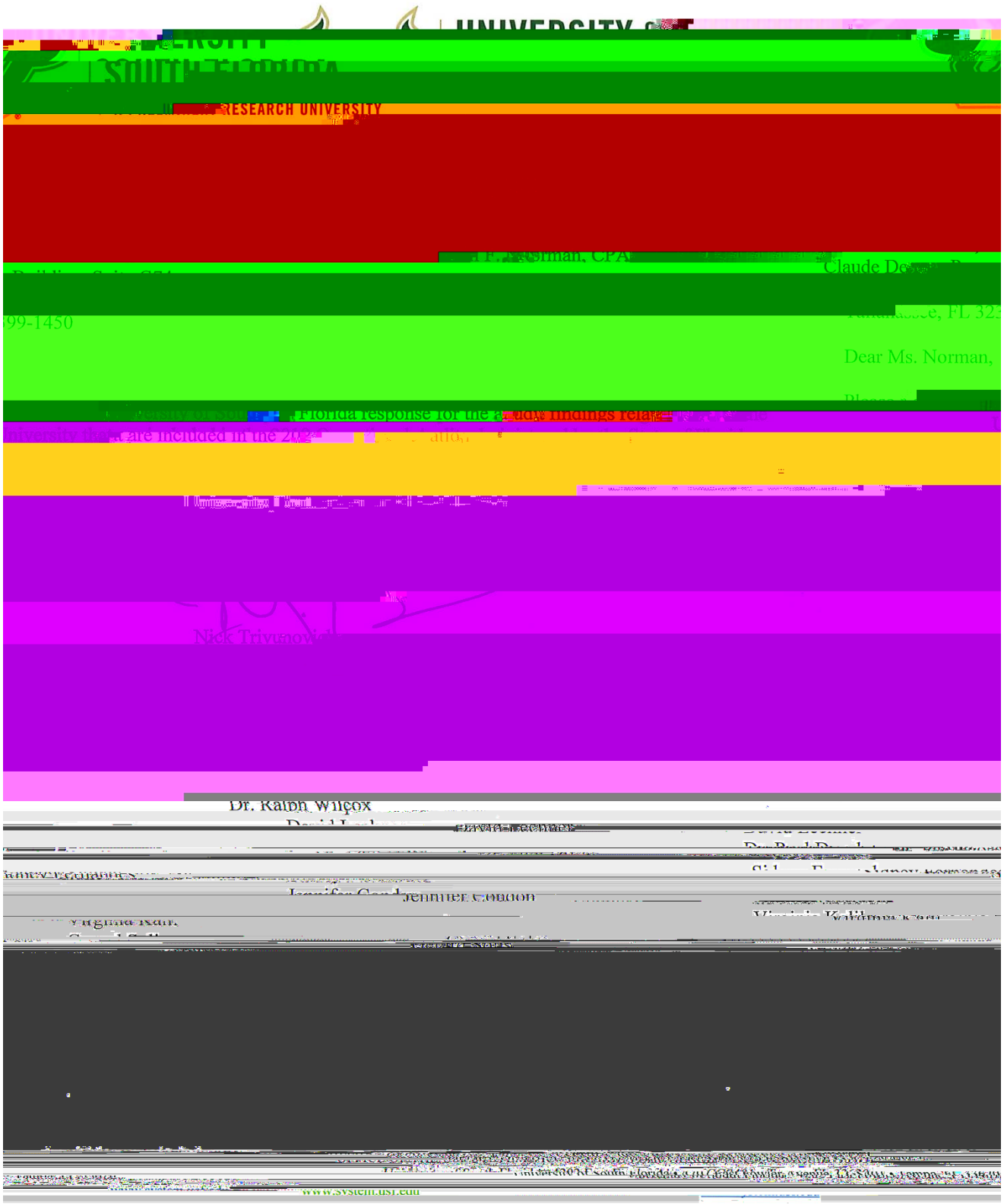
Reviewed the internal audit function to determine whether the University followed professional requirements and provided for peer review of reports issued. For internal audits, we determined whether audit reports were properly completed and submitted to the Trustees.

Examined University records to determine whether the University had developed an anti-fraud policy for the audit period to provide guidance to employees for communicating known or suspected fraud to appropriate individuals. Also, we examined University records to determine whether the University had implemented appropriate and sufficient procedures to comply with its anti-fraud pq m T R

M

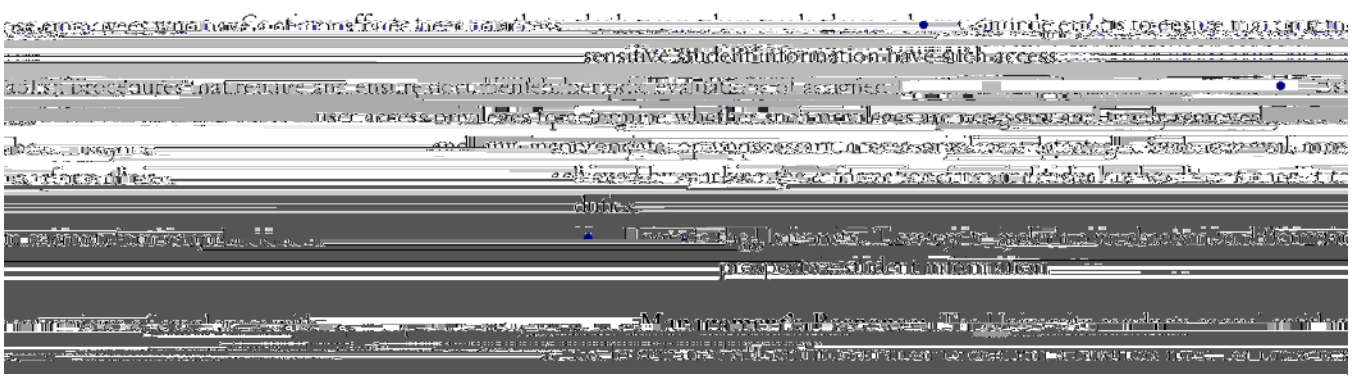
Analyzed payments from tuition differential fees collected during the audit period to determine whether the University assessed and used tuition differential fees in compliance with Section 1009.24(16)(a), Florida Statutes.

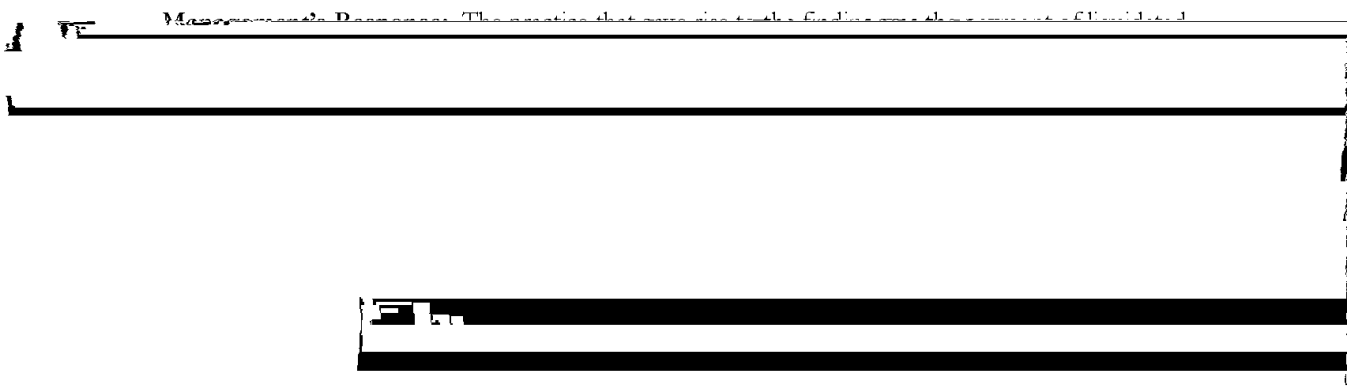
MANAGEMENT'S RESPONSE



Finding 1: Information Technology User Access Privileges – Social Security Numbers: Some

University should:





practice. As of the date of this letter we are not aware of any current, enforceable USF contract containing the former liquated damages provision.

Implementation Date:	December 1, 2016
Responsible Party:	Donna Keener, 813/974-5711