STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2016-033
November 2015

UNIVERSITY OF SOUTH FLORIDA

Data Center

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

Members of the University of South Florida Board of Trustees and the President who served during the period of our audit are listed below:

Harold W. Mullis, Jr., Chair
Brian D. Lamb, Vice Chair
Jean Cocco to 5-3-15 [a]
Jozef Gherman from 5-4-15 [a]
Stephanie E. Goforth
Scott L. Hopes
Stanley I. Levy
Stephen J. Mitchell
John B. Ramil
Debbie Nye Sembler
Byron E. Shinn
Gregory B. Teague [b]
Nancy H. Watkins
Jordan B. Zimmerman

Dr. Judy L. Genshaft, President

Notes: [a] Student body president.
[b] System faculty council president. Equivalent to faculty senate chair referred to in Section 1001.71(1), Florida Statutes.

The team leader was Benjamin Ho and the audit was supervised by Chris Gohlke, CPA, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General are available at:

www.myflorida.com/audgen

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 SOUTH FLORIDA

Data Center

SUMMARY

The University of South Florida (University) Data Center provides information technology (IT) services including application hosting for both the University and various customer entities. This operational audit focused on evaluating selected IT controls applicable to the University Data Center. As summarized below, the audit disclosed areas in which improvements in University Data Center controls and operational processes were needed.

Finding 1: Background screening controls for employees in positions of special trust needed improvement.

Finding 2: Certain IT security controls related to monitoring needed improvement.

BACKGROUND

Information technology (IT) services provided by the University of South Florida (University) Data Center include the hosting of student services, finance, and payroll applications for various customer entities, including the Florida Gulf Coast University, New College of Florida, and University of North Florida. The University hosts its student services application at the University Data Center.

FINDINGS AND RECOMMENDATIONS

Finding 1: Background Screening Controls

Effective security controls include the performance of background screenings for new employees and periodic rescreenings for current employees who are in positions of special trust. Such positions typically include IT employees with access privileges to, or responsibilities for the custody of, confidential or sensitive data and IT resources located within data centers. Additionally, University Policy 0-615, *Criminal History Background Checks*, requires that all prospective employees for positions designated as sensitive or special trust be subject to background screenings as a condition of employment.

We requested background screening documentation for 20 University employees with physical access privileges to the University Data Center as of April 28, 2015. University management did not provide background screening documentation for 6 employees. Five of the 6 employees had not been properly classified as holding positions of special trust, resulting in background screenings not being performed. In addition, our audit procedures disclosed that the University did not have procedures in place to perform periodic background rescreenings of all current employees in positions of special trust.

The absence of background screening documentation, improper classification of employees who are holding positions of special trust, and the lack of periodic background rescreenings for all applicable employees in positions of special trust increases the risk that persons with inappropriate backgrounds

may be employed or remain employed in positions of special trust and may gain access to confidential or sensitive data and IT resources.

Recommendation: University management should improve background screening controls to ensure that documentation relating to background screenings is maintained and that employees with physical access privileges to the University Data Center are properly classified as holding positions of special trust. Additionally, University management should establish procedures to perform periodic background rescreenings of all current employees in positions of special trust.

Finding 2: IT Security Controls - Monitoring

IT security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain University IT security controls related to monitoring needed improvement. We are not disclosing specific details of the issue in this report to avoid the possibility of compromising University data and IT resources. However, we have notified appropriate University management of the specific issue. Without adequate IT security controls related to monitoring, the risk is increased that the confidentiality, integrity, and availability of University data and IT resources may be compromised.

Recommendation: University management should improve IT security controls related to monitoring to ensure the continued confidentiality, integrity, and availability of University data and IT resources.

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 IT operational audit from April 2015 through July 2015 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to the University Data Center during the period April 2015 through June 2015. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources.
- To 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 the University Data Center systems and controls included within the scope of the audit, deficiencies in management's internal controls; instances of noncompliance with applicable governing laws, rules, or contracts; 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 IT controls, legal compliance matters, and records considered.

As described in more detail below, for the University Data Center systems and controls 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 the audit; obtaining an understanding of the University Data Center systems and controls; 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 the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This audit included the selection and examination of the University Data Center system controls and records. Unless otherwise indicated in this report, these items 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 agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting this audit, we:

- Interviewed University personnel.
- Obtained an understanding of the University Data Center's business processes related to contracting with customers for services.
- Obtained an understanding of physical access controls at the University Data Center, environmental safeguards, and the disaster recovery process, including backup procedures protecting IT resources.
- Obtained an understanding of the University Data Center's background screening controls and related processes.
- Observed and evaluated the effectiveness of physical access controls to the University Data Center.
- Observed and evaluated the effectiveness of University Data Center environmental safeguards in place to protect IT resources.
- Observed and evaluated the effectiveness of disaster recovery planning and testing and controls in place for the continuity of University Data Center operations, including proper tape backup and rotations and provisions for an off-site backup facility.
- Evaluated the appropriateness of access to the University Data Center. Specifically, we tested privileges for 109 University employees with physical access to the University Data Center as of April 28, 2015, to determine whether the employees had appropriate physical access privileges and authorizations.

- Evaluated the effectiveness of background screening controls to ensure that University management performed and periodically updated background screenings for University employees with physical access privileges to the University Data Center.
- Evaluated the effectiveness of IT security controls related to monitoring.
- 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, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

USF UNIVERSITY OF SOUTH FLORIDA.

November 4, 2015

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

Dear Ms. Norman:

Please find enclosed the University of South Florida System responses for the audit findings that are included in the Information Technology Operational Audit of the University of South Florida Data Center prepared by your office.

If you have any questions or require additional information, please contact Michael Sink, Senior Director and Technology Architect, at 813-974-3058.

Sincerely,

Sidney Fernandes
USF System Vice President/Chief Information Officer

Enclosure

Copy to: President Judy Genshaft, USF System
John Long, Chief Operating Officer and Sr. Vice President, Business and Finance
Calvin Williams, Vice President, Administrative Services
Michael Sink, Senior Director and Technology Architect
Donna Keener, Associate Vice President, Human Resources
Debra Gula, Executive Director, University Audit and Compliance

University of South Florida
Responses to Preliminary and Tentative Findings
Information Technology Operational Audit of the USF Data Center
Conducted by the Auditor General's Office

Finding No. 1: Background screening controls for employees in positions of special trust needed improvement.

Recommendation: University management should improve background screening controls to ensure that documentation relating to background screenings is maintained and that employees with physical access privileges to the University Data Center are properly classified as holding positions of special trust. Additionally, University management should establish procedures to perform periodic background re-screenings of all current employees in positions of special trust.

Management's Response: Management will perform background screenings of the six individuals identified in the audit report. Management is enhancing its procedures to ensure that background screening documentation is appropriately maintained and is implementing ongoing procedures to ensure that all USF Information Technology (USF IT) employees who hold a position of special trust are readily identifiable. Lastly, USF IT will work with USF Human Resources to implement procedures to ensure that periodic background re-screenings of USF IT employees in positions of special trust are performed.

Implementation Date: March 31, 2016

Responsible Party: Michael Sink, 813-974-3058

Finding No. 2: Certain IT security controls related to monitoring needed improvement.
Recommendation: University management should improve IT security controls related to monitoring to ensure the continued confidentiality, integrity, and availability of University data and IT resources.

Management's Response: The University has put measures in place to improve the monitoring of IT security controls identified by the State Auditor General to ensure the confidentiality, integrity, and availability of University data and IT resources.

Implementation Date: October 30, 2015

Responsible Party: Michael Sink, 813-974-3058