

STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-103
January 2019

FLORIDA POLYTECHNIC UNIVERSITY

Workday® Enterprise Cloud Applications



Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period July 2018 through October 2018, Dr. Randy K. Avent served as President of Florida Polytechnic University and the following individuals served as Members of the Board of Trustees:

Donald H. Wilson, Chair from 8-1-2018, Vice Chair through 7-31-2018	Dr. Richard P. Hallion
Clifford "Cliff" K. Otto, Vice Chair from 8-1-2018	Travis Hills ^b
Frank T. Martin, Chair though 7-31-2018	Henry McCance
R. Mark Bostick	Dr. Adrienne Perry
Dr. Jim Dewey ^a	Dr. Louis S. Saco
Rear Admiral Philip A. Dur, USN (Ret.)	Robert W. Stork
	Gary C. Wendt

^a Faculty Senate Chair.

^b Student Body President.

The audit was supervised by Heidi Burns, CPA, CISA.

Please address inquiries regarding this report to Heidi Burns, CPA, CISA, Audit Manager, by e-mail at heidiburns@aud.state.fl.us or by telephone at (850) 412-2926.

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

FLORIDA POLYTECHNIC UNIVERSITY

Workday® Enterprise Cloud Applications

SUMMARY

This operational audit of Florida Polytechnic University (University) focused on evaluating selected information technology (IT) controls applicable to the Workday® Enterprise Cloud Applications (Workday®), including the contractual relationship with Workday, Inc. as the provider for the University's Workday® Software as a Service subscription. As summarized below, our audit disclosed an area in which improvements in University controls and operational processes are needed.

Finding 1: University IT security controls related to account management need improvement.

BACKGROUND

The Florida Polytechnic University (University) is part of the State university system of public universities, which is under the general direction and control of the Florida Board of Governors (BOG). The University is directly governed by a Board of Trustees (Trustees) consisting of 13 members. The Governor appoints 6 citizen members and the BOG appoints 5 citizen members. These members are confirmed by the Florida Senate and serve staggered 5-year terms. The Faculty Senate Chair and Student Body President also serve as members.

While the BOG establishes the powers and duties of the Trustees, the Trustees are responsible for setting University policies, which are to provide governance in accordance with State law and BOG regulations. The Trustees select the University President, who is subject to confirmation by the BOG. The University President serves as the executive officer and the corporate secretary of the Trustees and is responsible for administering the University policies prescribed by the Trustees.

The University uses the Workday® Enterprise Cloud Applications (Workday®) for recording, processing, and reporting finance and human resources transactions. The University executed a Master Subscription Agreement (MSA) with Workday, Inc. on April 29, 2015, with an extended order effective April 29, 2018, for the subscription to Workday® using Software as a Service (SaaS). Under the terms of the MSA, Workday, Inc. hosts the Workday® applications and maintains and manages the supporting information technology (IT) infrastructure.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Controls – Account Management

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to account management

need improvement. We are not disclosing specific details of the issue in this report to avoid the possibility of compromising the confidentiality of University data and related IT resources. However, we have notified appropriate University management of the specific issue.

Without appropriate security controls related to account management, the risk is increased that the confidentiality, integrity, and availability of University data and related IT resources may be compromised.

Recommendation: **We recommend that University management improve IT security controls related to account management to ensure the 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 July 2018 through October 2018 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 University IT controls applicable to the Workday® Enterprise Cloud Applications, including those related to the University's contractual relationship with Workday, Inc. as the provider for the SaaS subscription during the period July 2018 through October 2018. The overall objectives of the audit were:

- To evaluate 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 IT 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 IT systems and controls included within the scope of this 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 IT 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 IT 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 University 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 and reviewed documentation applicable to University and Workday, Inc. operations to obtain and understanding of:
 - The delineation of responsibilities between the University and Workday, Inc. for the security, administration, support, and maintenance of Workday® and the supporting IT infrastructure, and the applicable contractual provisions.
 - IT infrastructure, including the hardware, operating systems, and database management system, as they relate to the support of the University's Workday® SaaS subscription.
 - Workday® controls that support the University's critical finance and human resources business processes.
- Evaluated the adequacy of University security management controls for ensuring the sufficiency of activities performed by Workday, Inc. related to data management and security.
- Evaluated the adequacy of University security management controls for ensuring the sufficiency of Workday, Inc. controls related to restricting administrative access privileges to the IT infrastructure supporting Workday®.
- Evaluated the adequacy of University security management controls for ensuring the sufficiency by which Workday, Inc. controls related to appropriateness of selected authentication controls for the IT infrastructure supporting Workday®.
- Evaluated the adequacy of University security management controls for ensuring the sufficiency of Workday, Inc. logging and monitoring controls over privileged administrator actions for the servers and databases that support Workday®.
- Evaluated the effectiveness of selected logical access controls for restricting administrative access privileges to the University's network domain.

- Evaluated the adequacy of the University's security management controls related to user authorization, periodic review of access, and the identification of sensitive transactions for Workday®.
- Evaluated the adequacy of system documentation relating to Workday® to promote efficient and effective operations.
- Evaluated the adequacy of the University's logging and monitoring controls over changes to the security and configuration of Workday®, including changes to user access, security group permissions, and business process rules.
- Evaluated the adequacy of the University's controls related to security group and business process rule creation, assignment, and ongoing maintenance.
- Examined and evaluated the adequacy of the University's controls over the security administration function for Workday®.
- Evaluated the appropriateness of selected authentication controls used to protect IT resources and University data for Workday®.
- Examined and evaluated the appropriateness of administrative privileges for the University's network domain as of July 24, 2018.
- Examined and evaluated access granted to eight critical Workday® business processes to determine if the processes enforce an appropriate separation of duties.
- 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



**FLORIDA POLYTECHNIC
UNIVERSITY**

Office of the President
Florida Polytechnic University
4700 Research Way
Lakeland, Florida 33805

January 11, 2019

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

Re: IT operational audit of Florida Polytechnic University, Workday® Enterprise Cloud Applications

Dear Ms. Norman:

The following is our response to the preliminary and tentative finding of your information technology operational audit of Florida Polytechnic University, Workday® Enterprise Cloud Applications.

Finding 1: Service Account Management

The University agrees with the finding and recommendation included in the report. We have taken appropriate corrective action to improve account security controls and ensure the confidentiality, integrity, and availability of University IT resources.

Sincerely,

A handwritten signature in black ink, appearing to read "Maver".

Dr. Randy K. Avent, Ph.D.
President
Florida Polytechnic University

4700 RESEARCH WAY | LAKELAND, FL | 33805-8531 | FLORIDAPOLY.EDU