Report No. 2023-186
April 2023

STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

FLORIDA POLYTECHNIC UNIVERSITY

Workday® Enterprise Cloud Applications

Sherrill F. Norman, CPA
Auditor General

Board of Trustees and President

During the period October 2021 through September 2022, Dr. Randy K. Avent served as President of Florida Polytechnic University and the following individuals served as Members of the Board of Trustees:

Clifford “Cliff” K. Otto, Chair
Beth Kigel, Vice Chair from 9-28-22
R. Mark Bostick, Vice Chair through 9-27-22
Dr. Ala J. Alnaser through 5-5-22 [a]
Samantha Ashby through 4-27-22 [b]
Dr. Narendra Kini
Dr. Susan LeFrancois from 5-6-22 [a]
Dr. Laine Powell
Melia Rodriguez from 4-28-22 [b]
Dr. W. Earl Sasser through 6-30-22 [c]
Lyn D. Stanfield
Robert “Bob” W. Stork
Gary C. Wendt

[a] Faculty Senate Chair.

[b] Student Body President.

[c] Trustee position was vacant 7-1-22, through 9-30-22.

Note: Two trustee positions were vacant for the entire period.

The team leader was George W. Phillips, CISSP, CISA, CFE, and 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 selected information technology (IT) controls applicable to the Workday® Enterprise Cloud Applications and the University's IT infrastructure, and a follow-up on findings noted in our report No. 2019-103. Our audit disclosed the following:

Finding 1: University security awareness training needs improvement to reduce the risk for University data to be compromised.

Finding 2: Certain University IT security controls related to authentication, data recovery, configuration management, account management, and vulnerability management need improvement to ensure the confidentiality, integrity, and availability of University data and IT resources. A similar finding related to account management was noted in our report No. 2019-103.

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 are also members. The BOG establishes the powers and duties of the Trustees. The Trustees are responsible for setting University policies, which provide governance in accordance with State law and BOG Regulations. The University President is selected by the Trustees and confirmed by the BOG. The University President serves as the executive officer and the corporate secretary of the Trustees and is responsible for administering the policies prescribed by the Trustees for the University.

The University uses the Workday® Enterprise Cloud Applications (Workday®) to record, process, and report finance and human resources transactions. Workday, Inc. hosts the University's subscription to Workday® using Software as a Service and maintains and manages the supporting infrastructure. The University uses the Comprehensive Academic Management Solution Enterprise system (CAMS®) to record student information. The University maintains and manages the network domain supporting access to Workday®, CAMS®, and University IT infrastructure.

FINDINGS AND RECOMMENDATIONS

Finding 1: Security Awareness Training

A comprehensive security awareness training program instructing all employees on the importance of preserving the confidentiality, integrity, and availability of data and IT resources entrusted to them is a

foundational control for security vigilance and a University's prevention and mitigation of cybersecurity risks. An effective security awareness program includes identification of the specific knowledge, skills, and abilities needed to support University security and educates all employees about how to interact with data and IT resources in a secure manner.

Our examination of University policies, procedures, and records supporting employee security awareness and skills training disclosed that the University had implemented mandatory training using a third-party provided software. Although the training addressed social engineering and security incident response, training on authentication and data handling best practices specific to University controls was not provided because the software could not be customized. In response to our inquiry, University management indicated on February 11, 2023, that options to add training customization would be further evaluated with the provider.

Effective security awareness training programs include authentication and data handling best practices and instructions to understand causes of unintentional data exposure. The lack of a comprehensive security awareness training program increases the risk that employees may compromise the confidentiality, availability, and integrity of University data and IT resources.

Recommendation: To reduce cybersecurity risks, University management should establish a comprehensive security awareness training program to ensure that employees are aware of their responsibilities and the importance of securing University data and IT resources.

Finding 2: Security Controls - Authentication, Data Recovery, Configuration Management, Account Management, and Vulnerability 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 authentication, data recovery, configuration management, account management, and vulnerability management need improvement. We are not disclosing specific details of the issues 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 six findings in the five areas needing improvement. A similar finding related to account management was noted in our report No. 2019-103.

Without appropriate security controls related to authentication, data recovery, configuration management, account management, and vulnerability 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 authentication, data recovery, configuration management, account management, and vulnerability management to ensure the confidentiality, integrity, and availability of University data and IT resources.

PRIOR AUDIT FOLLOW-UP

As discussed in Finding 2, the University had not taken corrective action for the finding included in our report No. 2019-103.

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 information technology (IT) operational audit from August 2022 through February 2023 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 significant University IT controls applicable to the Workday® Enterprise Cloud Applications (Workday®) and University IT infrastructure during the period October 2021 through September 2022, and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To determine the effectiveness of selected significant IT controls in achieving management's 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 determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2019-103.
- 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 included within the scope of the audit, deficiencies in management's internal controls that were significant to our audit objectives; 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 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 and evaluating the IT systems and related significant 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 agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, waste, abuse, or inefficiency.

In conducting this audit, we:

- Reviewed applicable laws, rules, and other guidelines to obtain an understanding of University organizational structure and regulatory requirements; reviewed University procedures, interviewed University personnel, and examined University records to obtain an understanding of University operations related to Workday® and IT infrastructure and to evaluate whether University operations were designed properly and operating effectively.
- Evaluated the sufficiency of University controls and observed, documented, and tested key processes, procedures, and controls related to Workday® and University IT infrastructure, including authentication, backup and recovery, configuration of systems, logical controls, and inventory and vulnerability management.
- Examined selected security settings related to University network infrastructure, externally facing applications, remote access systems, and other critical servers and devices to determine whether authentication controls were configured and enforced in accordance with IT best practices, including the use of multi-factor authentication.
- Evaluated the effectiveness of University logical access controls assigned to the University network and selected network devices, including the periodic evaluation of assigned accounts.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of August 30, 2022, within the four default network administrator system groups for the University root domain.
- Examined and evaluated, as of August 30, 2022, the 142 root domain accounts not required to have a password change.
- Examined and evaluated the appropriateness of all accounts assigned administrator access privileges, as of August 30, 2022, for the eight University high-risk network devices.
- Examined and evaluated the appropriateness of all accounts assigned selected administrative access privileges, as of August 26, 2022, to 10 of the 16 critical member servers in the University root domain.
- Examined and evaluated selected University patch management controls for operating systems and network devices to ensure secure configurations are maintained. Specifically, we examined and evaluated:
    - 22 critical servers as of November 16, 2022, and the additional 2 critical servers as of December 14, 2022.
    - The 8 high-risk network devices as of October 26, 2022.
- Evaluated University procedures and examined selected backup testing reports to determine the adequacy of the University data recovery procedures to restore University IT assets to a pre-incident trusted state.
- Evaluated the effectiveness of University configuration management controls, including establishing and maintaining secure configurations; disabling insecure protocols; implementing firewalls or port filtering to protect network resources; and timely applying software updates and managing device end-of-life.

- Evaluated University procedures and examined selected records to determine the adequacy of University procedures for maintaining a software asset inventory and ensuring only authorized software is installed on the network.
- Evaluated the effectiveness of University security awareness training.
- Evaluated University procedures and examined selected scan reports and policies to evaluate the adequacy of University vulnerability management controls related to the IT infrastructure, including vulnerability assessment and remediation, malicious software identification, and malware defense.
- 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

FLORIDA POLYTECHNIC UNIVERSITY

Office of the President
863-874-8612
president@floridapoly.edu

April 18, 2023

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

Dear Ms. Norman:

Pursuant to Section 11.45(4)(d), Florida Statutes, the university is required to submit a written statement of explanation concerning all findings. Please find the attached responses to the Preliminary and Tentative Findings for Florida Polytechnic University's *information technology operational audit of Workday® Enterprise Cloud Applications*. Should you have any questions, please contact Mr. David Blanton at (863) 874-8441.

Sincerely,

Dr. Randy K. Avent
President
Florida Polytechnic University

Florida Polytechnic University
Response to
Information Technology Operational Audit for Workday® Enterprise Cloud Applications
Audit Findings

Finding 1: Security Awareness Training

Recommendation: To reduce cybersecurity risks, University management should establish a comprehensive security awareness training program to ensure that employees are aware of their responsibilities and the importance of securing University data and IT resources.

Response: As noted in the finding, the University has in place mandatory security awareness training for all employees, covering areas such as social engineering and security incident response. The University will add training on authentication and data handling best practices as a standard feature of its training program.

Finding 2: Security Controls – Authentication, Data Recovery, Configuration Management, Account Management, and Vulnerability Management

Recommendation: We recommend that University management improve IT security controls related to authentication, data recovery, configuration management, account management, and vulnerability management to ensure the confidentiality, integrity, and availability of University data and IT resources.

Response: The University had already embarked on programs to improve several of the aspects covered in the finding at the time of the audit. The University will continue these efforts and expand them to include additional areas identified in the finding. The University will annually review these controls for compliance with best practices frameworks such as the *Center for Internet Security Critical Security Controls*.