STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2020-054
November 2019

FLORIDA STATE UNIVERSITY
NORTHWEST REGIONAL DATA CENTER

Data Center Operations

Sherrill F. Norman, CPA
Auditor General

Policy Board Members and Executive Director of the Northwest Regional Data Center

Florida State University is the administrative host institution and fiscal agent for the Northwest Regional Data Center (NWRDC). The NWRDC Charter establishes a Policy Board (Board), composed of customer entity representatives, as the governing body for the NWRDC. The Board's primary function is to establish and promulgate policies for the NWRDC. The Executive Director, who is appointed by the Board, is responsible for the overall administration of the NWRDC.

Tim Brown served as Executive Director of the NWRDC and the following individuals served as Board members during the period of our audit:

Board Member	Customer Entity Represented
Dr. Mehran Basiratmand, Chair	Small User Representative
Henry Martin, Vice Chair from 3-8-19	K-12 Representative
Michael Barrett to 3-7-19, Vice Chair to 3-7-19	Florida State University
Jesus Arias, Affiliate Member	Florida International University
Michael Dieckmann, Nonvoting Member from 7-7-18	University of West Florida
Ronald Henry, Nonvoting Member	Florida A&M University
Gene Kovacs	Board of Governors
Damu Kuttikrishnan	Florida Department of Revenue
Jane Livingston from 3-8-19	Florida State University
Dr. Andre Smith	Florida Department of Education
Sandra Stevens	City, County, and Local Government Representative

The team leader was Wayne Revell, CISA, and the audit was supervised by Hilda S. Morgan, CPA, CISA.

Please address inquiries regarding this report to Brenda Shiner, CISA, Audit Manager, by e-mail at brendashiner@aud.state.fl.us or by telephone at (850) 412-2946.

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 STATE UNIVERSITY
NORTHWEST REGIONAL DATA CENTER

Data Center Operations

SUMMARY

This operational audit of the Northwest Regional Data Center (NWRDC) focused on evaluating selected information technology (IT) controls applicable to data center operations and included a follow-up on the findings included in our report No. 2019-008. Our audit disclosed the following:

Finding 1: NWRDC management needs to improve policies and procedures to provide for the tracking and periodic inventory of IT resources. Similar findings were noted in prior audits of the NWRDC, most recently in our report No. 2019-008.

Finding 2: Certain NWRDC security controls related to physical access, logging and monitoring, and logical access need improvement to ensure the confidentiality, integrity, and availability of NWRDC customer entity data and related IT resources. Similar findings related to logical access were communicated to NWRDC management in connection with our prior audits of the NWRDC.

BACKGROUND

The Northwest Regional Data Center (NWRDC) is an auxiliary operation of Florida State University (University) and is headed by a Policy Board (Board) consisting of representatives from its customer entities. The Board appoints an Executive Director who is responsible for the daily operation of the data center. In its capacity as the administrative host institution and fiscal agent, the University is the contracting authority for the NWRDC and provides legal support and executive oversight. All NWRDC positions are filled with University employees who are to follow University payroll, leave, and other personnel policies.

The NWRDC provides a variety of information technology (IT) services to its customer entities, including facilities and infrastructure services, storage and recovery services, network and mainframe services, and security and other managed services. The NWRDC's customer entities consist of State agencies, universities, colleges, school districts, municipal and county governments, a consortium, and nonprofit entities that contract with the NWRDC for the aforementioned IT services. The NWRDC operates on a cost-recovery basis whereby the NWRDC bills the customer entities for its operating costs and allocates the billings based on the respective services provided to each customer. A list of the NWRDC customer entities is included in this report as ***EXHIBIT A***.

FINDINGS AND RECOMMENDATIONS

Finding 1: Inventory of IT Resources

Effective IT inventory controls include tracking and reconciling IT systems (e.g., physical and virtual servers) to ensure that management is knowledgeable of all IT systems for which they are responsible

and that the IT systems are configured as intended by management. Further, the tracking and periodic inventory of IT resources is necessary for effective monitoring, testing, and evaluation of IT resources to ensure the timely implementation of the latest relevant security patches and other critical updates (e.g., service packs and hot fixes) from IT vendors.

While the NWRDC *Policy and Procedure Manual* (*Manual*)[1] required tracking the receipt, reuse, and removal of hardware and electronic media, the *Manual* did not include policies and procedures requiring the tracking and periodic inventory of IT resources housed and maintained at the NWRDC. NWRDC staff maintained various manually prepared spreadsheets that contained information about the hardware and software assets within the data center and indicated that they were in the process of configuring an asset discovery tool to scan the NWRDC IT environment nightly for use in generating a hardware and software asset listing of IT resources maintained and housed at the NWRDC. While NWRDC management provided the results of a nightly scan performed on April 10, 2019, NWRDC management stated the processes to reconcile the spreadsheet information to the hardware and software asset listing generated from the scan were still in development.

Appropriate IT resource tracking and inventory procedures that include reconciliations of IT resources to asset listings facilitate complete, accurate, and up-to-date records necessary to ensure that management is knowledgeable of all IT systems for which they are responsible, the IT systems are configured as intended by management, and the timely implementation of the latest relevant security patches and other critical updates from IT vendors. Similar findings were noted in prior audits of the NWRDC, most recently in our report No. 2019-008.

Recommendation: We again recommend that NWRDC management establish a documented process, with corresponding policies and procedures, for tracking IT resources and periodically reconciling and documenting the IT resource inventory to asset listings and other applicable NWRDC records.

Finding 2: Security Controls – Physical Access, Logging and Monitoring, and Logical Access

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain NWRDC security controls related to physical access, logging and monitoring, and logical access need improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising NWRDC customer entity data and related IT resources. However, we notified appropriate NWRDC management of the specific issues.

Without appropriate security controls related to physical access, logging and monitoring, and logical access, the risk is increased that the confidentiality, integrity, and availability of customer entity data and related IT resources may be compromised. Similar findings related to logical access were communicated to NWRDC management in connection with prior audits of the NWRDC, most recently with our report No. 2019-008.

[1] NWRDC *Policy and Procedure Manual, Section 7.80, Tracking Reassignment/Movement of Inventories*, effective April 10, 2019.

Recommendation: We recommend that NWRDC management improve certain security controls related to physical access, logging and monitoring, and logical access to ensure the confidentiality, integrity, and availability of NWRDC customer entity data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the NWRDC had taken corrective actions for the findings included in our report No. 2019-008.

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 March 2019 through June 2019 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 Northwest Regional Data Center (NWRDC) operations during the period July 2018 through June 2019 and selected actions subsequent thereto. 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 at the NWRDC.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2019-008.
- 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 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 NWRDC personnel and reviewed NWRDC documentation to obtain an understanding of:
    - The NWRDC hardware and software tracking and reconciliation procedures used to ensure a complete and up-to-date inventory of IT resources.
    - The IT infrastructure and architecture of the NWRDC, including the hardware, operating systems and versions for the various server and hardware platforms and the hardware, operating systems and versions, and security software and versions for the network components.
    - The methods for authenticating to the NWRDC systems and the interconnected network.
    - The statutory and contractual requirements, customers served, and services offered by the NWRDC.
    - Processes for granting, discontinuing, periodic reviewing, logging, and monitoring physical access to the data center facilities for NWRDC employees, customers, vendors, and visitors.
- Evaluated the inventory and tracking controls including periodic reconciliations for ensuring the completeness and accuracy of the manually generated inventory spreadsheets maintained by the NWRDC.
- Evaluated the logical access controls for 15 of the 103 mainframe accounts with elevated privileges (administrative accounts) as of May 23, 2019, to determine whether the accounts were necessary.
- Evaluated the periodic review policies, procedures, and processes and examined NWRDC records for the performance of periodic access reviews of logical access privileges to NWRDC IT resources.
- Evaluated user authentication controls for the NWRDC IT infrastructure.
- Evaluated configuration management policies, procedures, and processes for ensuring that IT resources and customer-entity data are properly protected.
- Evaluated logical access and override controls for the employee time tracking system used for customer billing functions. Specifically, we examined the four Harvest user accounts assigned *Administrator* access privilege as of April 12, 2019, to determine whether the assigned access was based on job responsibilities and promoted an appropriate separation of duties.

- Evaluated NWRDC security controls for protecting IT resources and data, including the appropriateness and review of physical access and logging and monitoring of physical access to the data center and sensitive areas. Specifically, we:
  - Evaluated the appropriateness of physical access privileges for the 50 active user access badges as of April 26, 2019, that allowed access to sensitive areas within the data center.
  - Evaluated policies, procedures, and processes and examined NWRDC records to determine whether adequate logging and monitoring controls existed.
  - Evaluated policies, procedures, and processes associated with the periodic review of physical access for employees and customers, including access to sensitive areas within the data center.
- 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

EXHIBIT A

NWRDC CUSTOMER ENTITIES

AS OF JULY 10, 2019

Higher Education Entities

Chipola College	Florida State University	University of Central Florida
Florida A&M University	Florida Virtual Campus	University of Florida
Florida Atlantic University	Miami Dade College	University of North Florida
Florida Center for Interactive Media at Florida State University	New College of Florida	University of South Florida
Florida Gulf Coast University	Palm Beach State College	University of West Florida
Florida International University		

State Agencies and Other Government Entities

Board of Governors	Department of Highway Safety and Motor Vehicles	Early Learning Coalition of the Emerald Coast
Department of Business and Professional Regulation	Department of Revenue	Florida Prepaid College Board
Department of Education	Department of State	Office of Early Learning, Department of Education
Department of Financial Services	Division of State Technology, Department of Management Services	Statewide Guardian Ad Litem
Department of Health		

K-12 School Districts

Alachua County District School Board	Florida Virtual School	Panhandle Area Educational Consortium:
Bay County District School Board	Hillsborough County District School Board	Calhoun County District School Board
Columbia County District School Board	Miami-Dade County District School Board	Florida A&M University Developmental Research School
DeSoto County District School Board	Nassau County District School Board	Franklin County District School Board
Escambia County District School Board	Palm Beach County District School Board	Gadsden County District School Board
Florida Atlantic University Schools	Santa Rosa County District School Board	Gulf County District School Board
Florida School for the Deaf and the Blind	St. Johns County District School Board	Holmes County District School Board
Florida State University Schools	Suwannee County District School Board	Jackson County District School Board
		Jefferson County District School Board
		Liberty County District School Board
		Madison County District School Board
		Taylor County District School Board
		Wakulla County District School Board
		Walton County District School Board
		Washington County District School Board

Local Government, Health Care, and Other Entities

City of Boca Raton	Florida State University Health Services	Palm Beach County Board of County Commissioners
City of Delray Beach	Health Care District of Palm Beach County	Palm Beach County Clerk and Comptroller
City of Jacksonville	Leon County Government	Tallahassee Memorial HealthCare, Inc.
City of West Palm Beach	Orange County Board of County Commissioners	The Ringling Museum of Art, Florida State University
Florida State University Foundation	Orange County Clerk of Courts	

Source: Diana Norwood, Associate Director, Administrative Services, NWRDC.

MANAGEMENT'S RESPONSE

NWRDC
Northwest Regional Data Center

2048 East Paul Dirac Drive
Tallahassee, FL 32310-3752
850.645.3500 Phone
850.645.3570 Fax

Sherrill F. Norman
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450
November 12, 2019

Dear Ms. Norman,

Please accept Florida State University's response to your October 10th letter regarding the recent audit of Northwest Regional Data Center. As always, please let us know if there are any questions or if we can be of any assistance. Thank you.

Sincerely,

Tim Brown
Executive Director, Northwest Regional Data Center
Florida State University

Cc:
Sam McCall, Chief Audit Officer, Florida State University
Mehran Basiratmand, CTO, Florida Atlantic University; Chair, NWRDC Policy Board
Jane Livingston, Assoc. VP & CIO, Florida State University

Public Finding 1: NWRDC management needs to improve policies and procedures to provide for the tracking and periodic inventory of IT resources. Similar findings were noted in prior audits of the NWRDC, most recently in our report No. 2019-008.

Recommendation: We again recommend that NWRDC management establish a documented process, with corresponding policies and procedures, for tracking IT resources and periodically reconciling and documenting the IT resource inventory to asset listings and other applicable NWRDC records.

NWRDC Response: NWRDC has established a documented policy and procedure to reconcile NWRDC's IT resources with asset listings and other NWRDC records. An initial inventory reconciliation was performed in August 2019, NWRDC policy was revised in October 2019 to require a quarterly manual IT inventory reconciliation of device inventories against reports from NWRDC's network discovery tool, and a second inventory reconciliation is currently underway as of November 2019.

Public Finding 2: Certain NWRDC security controls related to physical access, logging and monitoring, and logical access need improvement to ensure the confidentiality, integrity, and availability of NWRDC customer entity data and related IT resources. Similar findings related to logical access were communicated to NWRDC management in connection with our prior audits of the NWRDC.

Recommendation: We recommend that NWRDC management improve certain security controls related to physical access, logging and monitoring, and logical access to ensure the confidentiality, integrity, and availability of NWRDC customer entity data and related IT resources.

NWRDC Response: NWRDC has improved security controls related to logging and monitoring, and logical access as recommended in the detailed confidential audit report for these areas. Regarding physical access, NWRDC management met with its Policy Board during the most recent quarterly meeting, held on November 8th, 2019, and presented the Auditor General's specific concerns regarding data center access for employees. The NWRDC Policy Board concluded that the current policy and process for granting employee access is acceptable. Management has also implemented a formal monthly building access review of all security door activity as an additional control for employee physical access.