STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2023-045
November 2022

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 Users
Gene Kovacs, Vice Chair	Board of Governors
Dr. Jesus Arias, Nonvoting Member	Institutional Affiliate
Dr. Rick Burnette	Florida State University
Paul Chafin	Florida Department of Health
Damu Kuttikrishnan, to 10-12-21	Florida Department of Revenue
Jimmie Harrell, from 10-29-21	Florida Department of Revenue
Robert Seniors, Nonvoting Member	Florida A&M University
Dr. Andre Smith	Florida Department of Education
Sandra Stevens	City, County, and Local Governments
Vacant, Nonvoting Member	University of West Florida

The audit was supervised by Suzanne Varick, CPA.

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 significant information technology (IT) controls applicable to data center operations and included a follow-up on the findings included in our report No. 2021-146. Our audit disclosed the following:

Finding 1: NWRDC periodic access review controls continue to need improvement.

Finding 2: Certain NWRDC security controls related to vulnerability management, user authentication, and encryption need improvement to ensure the confidentiality, integrity, and availability of NWRDC and customer entity data and related IT resources.

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 operations 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.

The NWRDC provides a variety of information technology (IT) services to its customer entities, including facilities, infrastructure, storage and recovery, network, mainframe, 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: Periodic Review of Access Privileges

Periodic reviews of user and service accounts with access to data and IT resources help protect the confidentiality, integrity, and availability of data and IT resources by ensuring that only authorized users have access and that the access privileges assigned to user and service accounts remain appropriate and necessary. An effective periodic review consists of identifying the current access privileges of system users and services and evaluating the assigned access privileges to ensure that they align with user job responsibilities or service account requirements.

To facilitate the periodic review of employee accounts and the assigned access privileges, the NWRDC *Policy and Procedure Manual* (*Manual*) required employee accounts and privileges (logical access for IT devices, systems, and applications) be reviewed annually in accordance with documented procedures and for validity and appropriateness based on an employee's role and the principles of least privilege and need to know. The *Manual* also required, at a minimum, an annual review of privileged service accounts and accounts that were not assigned to a specific individual for validity and business need. In our report No. 2021-146 (Finding 2), we noted that NWRDC access review procedures were in the process of being revised and did not align with either the *Manual* or NWRDC review processes. As part of our current audit, we noted that, while the *NWRDC User Access Control Review Procedure* (*Procedure*) was updated in January 2022, as of March 2022, access reviews for user and service accounts had not been completed since July 10, 2020. In response to our audit inquiry, NWRDC management indicated that they had delayed performing the periodic access reviews while the *Procedure* was being updated.

Comprehensive periodic access reviews ensure that access privileges granted to users are authorized by management and that user and service accounts are restricted to access privileges needed for the accomplishment of the users' assigned job responsibilities and service account requirements.

Recommendation: We recommend that NWRDC management ensure that comprehensive periodic reviews of the appropriateness of user and service account access privileges are conducted in accordance with the *Manual*.

Finding 2: Security Controls – Vulnerability Management, User Authentication, and Encryption

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 vulnerability management, user authentication, and encryption need improvement to ensure the confidentiality, integrity, and availability of NWRDC and customer entity data and related IT resources. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising NWRDC and customer entity data and related IT resources. However, we have notified appropriate NWRDC management of the three findings in the areas needing improvement.

Without appropriate security controls related to vulnerability management, user authentication, and encryption, the risk is increased that the confidentiality, integrity, and availability of NWRDC and customer entity data and related IT resources may be compromised. Similar findings related to vulnerability management and user authentication were communicated to NWRDC management in connection with our report No. 2021-146.

Recommendation: We recommend that NWRDC management improve certain security controls related to vulnerability management, user authentication, and encryption to ensure the confidentiality, integrity, and availability of NWRDC and 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. 2021-146.

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 December 2021 through June 2022 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 IT controls applicable to Northwest Regional Data Center (NWRDC) operations during the period July 2021 through April 2022 and selected actions subsequent thereto. For those areas addressed by this audit, our audit objectives were:

- To evaluate the effectiveness of selected significant 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 determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2021-146.
- 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, NWRDC policies and procedures, and other guidelines, and interviewed NWRDC personnel to obtain an understanding of the NWRDC organizational structure, statutory requirements, and operational processes.
- Interviewed NWRDC personnel and examined NWRDC records to obtain an understanding of the NWRDC network infrastructure and related hardware, software, and authentication methods, data center services provided, and customers served.
- Interviewed NWRDC personnel and examined NWRDC records to obtain an understanding of NWRDC processes for approving, assigning, deactivating, and reviewing administrative-level access to the mainframe; IT asset management, including periodic reconciliation of IT asset records; vulnerability management, including vulnerability scanning, analysis, and remediation; restricting physical access to NWRDC facilities and sensitive IT resources, including granting, discontinuing, logging, and periodically reviewing physical access to NWRDC facilities and sensitive IT resources; and disaster recovery, including customer entity disaster recovery offerings.
- Examined NWRDC IT asset management policies, procedures, and records and evaluated the adequacy of IT asset management processes for recording and periodically reconciling NWRDC IT asset records. Specifically, we examined the IT asset reconciliation performed for the quarter ended December 2021 to determine whether the reconciliation was sufficient, including whether the reconciliation identified discrepancies by comparing asset discovery tool records to configuration management database inventory records and whether identified discrepancies were promptly investigated and resolved.
- Evaluated the logical access controls for the mainframe administrative-level accounts, including whether customer accounts were adequately restricted from other customer entity mainframe resources. Specifically, we evaluated the appropriateness of the administrative-level access privileges for 15 of the 53 active NWRDC mainframe accounts as of February 14, 2022.
- Evaluated the adequacy of periodic review policies, procedures, and processes for logical access privileges for NWRDC IT devices, systems, and applications.
- Evaluated the appropriateness of physical access controls for the NWRDC, including the adequacy of policies, procedures, and processes established to protect sensitive IT areas. Specifically, we:
    - Observed physical access controls to the NWRDC, including sensitive IT areas, as of February 3, 2022.
    - Evaluated the appropriateness of physical access privileges to sensitive IT areas assigned to the 44 key cards active as of February 3, 2022.
    - Examined NWRDC records to determine the adequacy of the December 2021 review of physical access privileges and door entry logs to the sensitive IT areas.
- Evaluated the adequacy of selected NWRDC IT infrastructure authentication controls.
- Evaluated the adequacy of NWRDC vulnerability management policies and procedures and the effectiveness of vulnerability management processes, including the timely performance of

authenticated scans and the timely communication, analysis, and remediation of identified vulnerabilities for the NWRDC network infrastructure, mainframe, Windows, open systems, and disaster recovery environments.

- Evaluated the adequacy of NWRDC Web site security controls.
- Evaluated the adequacy of NWRDC disaster recovery policies, procedures, and processes, including whether an up-to-date disaster recovery plan was maintained and tested annually and whether an alternative data center facility and related infrastructure were available in the event of a disaster or other interruption of service.
- 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 JUNE 30, 2022

Higher Education Entities

Broward College	Florida State University	State College of Florida, Manatee-Sarasota
Florida A&M University	Florida Virtual Campus	University of Central Florida
Florida Atlantic University	Gulf Coast State College	University of Florida
Florida Center for Interactive Media at Florida State University	New College of Florida	University of North Florida
Florida Gulf Coast University	Palm Beach State College	University of South Florida
Florida International University	Polk State College	University of West Florida
Florida Polytechnic University		

State Agencies and Other Government Entities

Board of Governors	Department of Juvenile Justice	Early Learning Coalition of the Emerald Coast
Department of Business and Professional Regulation	Department of the Lottery	Florida Commission on Human Relations
Department of Education	Department of Management Services	Florida Digital Service, Department of Management Services
Department of Financial Services	Department of Revenue	Florida Prepaid College Board
Department of Health	Department of State	Statewide Guardian Ad Litem
Department of Highway Safety and Motor Vehicles		

K-12 School Districts

Bay County District School Board	Miami-Dade County District School Board	Panhandle Area Educational Consortium: Calhoun County District School Board Florida A&M University Developmental Research School Franklin County District School Board Gadsden County District School Board Gulf County District School Board Holmes 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
Columbia County District School Board	Monroe County District School Board	
Escambia County District School Board	Nassau County District School Board	
Florida Atlantic University Schools	Palm Beach County District School Board	
Florida School for the Deaf and the Blind	Pinellas County District School Board	
Florida State University Schools	Santa Rosa County District School Board	
Florida Virtual School	St. Johns County District School Board	
Hillsborough County District School Board	Suwannee County District School Board	
Manatee County District School Board		

Local Government, Health Care, and Other Entities

Alachua County Government	City of Jacksonville	Palm Beach County Board of County Commissioners
Big Bend Hospice	Florida State University Foundation	Palm Beach County Clerk and Comptroller
City of Boca Raton	Health Care District of Palm Beach County	Palm Beach County Department of Health
City of Boynton Beach	Hernando County Clerk of Circuit Court and Comptrollers	Palm Beach County Office of the Public Defender
City of Coral Springs	Miami-Dade County Government	Tallahassee Memorial HealthCare, Inc.
City of Delray Beach	Orange County Clerk of Courts	The Ringling Museum of Art, Florida State University

Source: NWRDC personnel.

NWRDC
FLORIDA'S CLOUD BROKER

FL VC FLORIDA VIRTUAL CAMPUS

October 24, 2022

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

Dear Mrs. Norman:

Please accept Florida State University's response to your letter of September 27th with a report of preliminary and tentative findings and recommendations from your recent Northwest Regional Data Center audit. As always, please let us know if there are any questions or if we can be of assistance. Thank you.

Sincerely,

Tim Brown
Assistant Vice President for IT Services
NWRDC & FLVC
Florida State University

Cc: Undra Baldwin, Chief Audit Officer, Florida State University

2048 East Paul Dirac Drive
Tallahassee, FL 32310-3752
850.645.3500
info@nwrdc.fsu.edu
www.nwrdc.fsu.edu
www.flvc.org

Finding #1: Periodic Review of Access Privileges

Recommendation:

We recommend that NWRDC management ensure that comprehensive periodic reviews of the appropriateness of user and service account access privileges are conducted in accordance with the Manual.

NWRDC Response:

NWRDC management has ensured that comprehensive periodic reviews of the appropriateness of user and service account access privileges are being conducted. On January 21, 2022, NWRDC implemented IT Access Management 7.90, located within NWRDC's policy manual. Since its implementation, NWRDC has conducted three comprehensive access management reviews, with a fourth in progress.

Finding #2: Security Controls – Vulnerability Management, User Authentication, and Encryption

Recommendation:

We recommend that NWRDC management improve certain security controls related to vulnerability management, user authentication, and encryption to ensure that confidentiality, integrity, and availability of NWRDC and customer entity data and related IT resources.

NWRDC Response:

NWRDC management was executing a project upon commencement of the audit and will continue to implement others that will enhance security controls related to vulnerability management, user authentication, and encryption to ensure that confidentiality, integrity, and availability of NWRDC and customer entity data and related IT resources. We will continuously improve our security controls as recommended.

2048 East Paul Dirac Drive
Tallahassee, FL 32310-3752
850.645.3500
info@nwrdc.fsu.edu
www.nwrdc.fsu.edu
www.flvc.org