STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2019-008
August 2018

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
Michael Barrett, Vice Chair and Management Committee Chair	Florida State University
Ronald Henry, Non-Voting Member	Florida A&M University
Michael Dieckmann	University of West Florida
Ted Duncan through 4-27-18	Florida Department of Education
Levis Hughes, Management Committee Member through 4-27-18	Florida Department of Education
Dr. Andre Smith from 4-27-18	Florida Department of Education
Gene Kovacs	State University System of Florida, Board of Governors
Henry Martin, Management Committee Member	K-12 Representative
Damu Kuttikrishnan	Florida Department of Revenue
Sandra Stevens from 2-3-18	City, County, and Local Government Representative
Jesus Arias, Affiliate Member	Florida International University

The team leader was Benjamin Ho, CISA, and the audit was supervised by Hilda 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. 2018-003. 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. A similar finding was noted in report No. 2018-003.

Finding 2: As similarly noted in report No. 2018-003, the NWRDC did not perform comprehensive periodic reviews of access privileges for the Windows server, Linux server, network, and mainframe environments.

Finding 3: Some access privileges did not promote an appropriate separation of duties.

Finding 4: Certain NWRDC security controls related to logical access, user authentication, and configuration management for NWRDC resources continue to need improvement to ensure the confidentiality, integrity, and availability of NWRDC customer entity data and related IT resources. Similar findings related to logical access, user authentication, and configuration management were communicated to NWRDC management in connection with our report No. 2018-003.

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 and for-profit 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.

As part of our audit procedures we determined that, 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 used a vulnerability assessment tool to quarterly scan the NWRDC IT environment and generate a hardware and software asset listing of IT resources maintained and housed at the NWRDC. While NWRDC management provided the results of a scan performed on February 16, 2018, as of April 22, 2018, NWRDC management was unable to provide documentation detailing a reconciliation of the spreadsheet information to the hardware and software asset listings generated from the February 16, 2018, scan to ensure that the information in the various spreadsheets was complete and up-to-date.

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. A similar issue was noted in our report No. 2018-003.

Recommendation: We 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: Periodic Review of Access Privileges

Effective access controls include periodic reviews of user access privileges and system service accounts to ensure accounts remain appropriate to protect the confidentiality, integrity, and availability of data and IT resources. Additionally, periodic reviews of user accounts to data and IT resources help ensure that only authorized users have access and that the access provided to each user remains appropriate and necessary for the user's assigned job duties.

[1] NWRDC *Policy and Procedure Manual, Section 7.80, Tracking Reassignment/Movement of Inventories,* effective October 27, 2017.

Our review disclosed that the *Manual* did not contain specific information regarding the method and frequency of required periodic reviews of access privileges. Additionally, NWRDC management stated that while a comprehensive periodic review was in progress as of May 2, 2018, for the Windows server, Linux server, network, and mainframe environments, a comprehensive periodic review, including remediation of access privileges deemed no longer necessary, had not been completed.

Without procedures establishing the method and frequency of periodic reviews of all access privileges, and documentation of such reviews, management's assurance that access privileges were authorized and appropriate is limited. A similar issue was noted in our report No. 2018-003.

Recommendation: We recommend that NWRDC management revise procedures to provide for comprehensive periodic reviews of access privileges to ensure that access privileges are authorized and appropriate. Such procedures should establish the method and frequency of reviews.

Finding 3: Appropriateness of Access Privileges

Effective access controls include measures to restrict access privileges to data and IT resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. Appropriately restricting the use and access capabilities of accounts helps protect the confidentiality, integrity, and availability of data and IT resources.

To facilitate customer billings, the NWRDC uses Harvest, a Web-based application for employee time tracking to attribute billable hours to specific customers. Employee time tracking information recorded in Harvest is periodically reviewed and customer billing rates adjusted as necessary. Additionally, the NWRDC uses QuickBooks Online for financial and management accounting, including customer billing functions.

While Harvest users assigned the *Employee* access privilege were restricted to recording their own time, users assigned the *Administrator* access privilege, in addition to recording their own time, were also allowed to record or update time for any employee listed in the Harvest application. As part of our audit procedures, we evaluated the seven Harvest user accounts assigned the *Administrator* access privilege and the three NWRDC QuickBooks Online user accounts, as of December 13, 2017, to determine whether the assigned access promoted an appropriate separation of duties and was necessary for the user's assigned job duties. Our audit procedures disclosed that one user was assigned both a Harvest user account with the *Administrator* access privilege and a QuickBooks Online user account, contrary to an appropriate separation of duties.

Access to incompatible and inappropriate functions, such as access that allows the same user to update employee time records in the Harvest application and adjust customer billings in QuickBooks Online, increases the risk of misappropriation of assets and erroneous manipulation of data.

Recommendation: We recommend that NWRDC management ensure that assigned user access privileges promote an appropriate separation of duties.

Finding 4: Security Controls – Logical Access, User Authentication, and Configuration Management

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 logical access, user authentication, and configuration management 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 logical access, user authentication, and configuration management, 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, user authentication, and configuration management were communicated to NWRDC management in connection with our report No. 2018-003.

Recommendation: We again recommend that NWRDC management improve certain security controls related to logical access, user authentication, and configuration management 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. 2018-003.

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 November 2017 through April 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 NWRDC IT controls applicable to NWRDC operations during the period July 2017 through April 2018 and selected actions subsequent thereto. 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 at the NWRDC.

- To determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2018-003.
- 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 NWRDC 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 NWRDC 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 NWRDC 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 NWRDC 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 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, software, and operating systems and versions, related to the various server platforms and the hardware, operating systems and versions, and security software and versions related to the network components.
  - The logging and monitoring capabilities and review functions at the NWRDC related to the capture and review of system activity, including access to and modifications of IT resources at the NWRDC.
  - The user provisioning and periodic review processes for logical access to NWRDC systems and the interconnected network, including any user provisioning requirements for customer accounts.

- The methods for authenticating to the NWRDC systems and the interconnected network.
- The patch management process for the mainframe, firewalls, Linux servers, and Windows servers.
- The statutory and contractual requirements, customers served, and services offered by the NWRDC.

- Evaluated the inventory and tracking controls for ensuring the completeness and accuracy of the manually generated inventory spreadsheets maintained by the NWRDC by comparing the system-generated inventory map to the inventory spreadsheets. Specifically, we evaluated the map results from the vulnerability assessment tool as of February 16, 2018, to determine whether the IT assets identified on the system-generated inventory map were completely and accurately accounted for on the inventory spreadsheets.
- Evaluated the effectiveness of the NWRDC patch management processes for the mainframe and high-risk network devices. Specifically, we examined:
  - The mainframe production logical partition as of February 12, 2018, to evaluate whether the NWRDC had timely installed vendor-suppled patches.
  - The 6 high-risk network devices as of February 9, 2018, to evaluate whether the NWRDC had timely installed vendor-supplied patches.
- Evaluated the effectiveness of NWRDC logging and monitoring controls.
- Evaluated the NWRDC policies and procedures for storing and disposing of storage media.
- Evaluated the logical access controls for administrative accounts and periodic review procedures for logical access privileges to NWRDC IT resources. Specifically, we evaluated:
  - The appropriateness of administrative access privileges for the 1 network domain used for NWRDC services and operations as of February 8, 2018.
  - The appropriateness of access privileges for 31 selected mainframe environment administrative accounts as of February 26, 2018.
- Evaluated user authentication controls related to the NWRDC IT infrastructure.
- Evaluated logical access, authentication, and override controls for the employee time tracking system used to facilitate customer billings. Specifically, we examined the 7 Harvest user accounts assigned the *Administrator* access privilege and the 3 NWRDC QuickBooks Online user accounts as of December 13, 2017, to determine whether the assigned access promoted an appropriate separation of duties and was necessary for the user's assigned job 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

EXHIBIT A

NWRDC CUSTOMER ENTITIES

AS OF MAY 29, 2018

Higher Education Entities

Chipola College	Florida State College of Jacksonville	Santa Fe College
College of Central Florida	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 Gateway College	Palm Beach State College	University of West Florida
Florida Gulf Coast University	Pensacola State College	
Florida International University	Polk State College	

State Agencies and Other Government Entities

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

K-12 School Districts

Alachua County District School Board	Lee County District School Board	Panhandle Area Educational Consortium:
Bay County District School Board	Manatee County District School Board	Calhoun County District School Board
Columbia County District School Board	Miami-Dade County District School Board	Franklin County District School Board
Desoto County District School Board	Nassau County District School Board	Florida A&M University Developmental Research School
Escambia County District School Board	Palm Beach County District School Board	Gadsden County District School Board
Florida Atlantic University Schools	Pinellas County District School Board	Gulf County District School Board
Florida School for the Deaf and the Blind	Santa Rosa County District School Board	Holmes County District School Board
Florida State University Schools	St. Johns County District School Board	Jackson County District School Board
Florida Virtual School	Suwannee County District School Board	Jefferson County District School Board
Hillsborough 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 Delray Beach	Florida State University Health Services	Palm Beach County Board of County Commissioners
City of Boca Raton	Health Care District of Palm Beach County	Palm Beach County Clerk and Comptroller
City of Jacksonville	Leon County Government	Tallahassee Memorial HealthCare, Inc.
Conduent Healthcare Knowledge Solutions, Inc.	Orange County Clerk of Courts	The Ringling Museum of Art, Florida State University
Florida State University Foundation	Orange County Board of County Commissioners	

Source: Tim Brown, Executive Director, NWRDC.

MANAGEMENT'S RESPONSE

NWRDC™
Northwest Regional Data Center

2048 East Paul Dirac Drive
Tallahassee, FL 32310-3752
850.245.3500 Phone
850.245.3570 Fax

Sherrill F. Norman
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450
July 31, 2018

Dear Ms. Norman,

Please accept Florida State University's response to your July 2nd 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
Michael Barrett, Assoc. VP & CIO, Florida State University; Vice-Chair of NWRDC Policy Board
Mehran Basiratmand, CTO, Florida Atlantic University; Chair of NWRDC Policy Board

NWRDC Response

Finding 1: Inventory of IT Resources
Recommendation: We 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: While NWRDC agrees with this recommendation and that there is still work to be done, NWRDC has made considerable improvements in this area during the past audit cycle. The tool that is referenced in the audit report is for security management and was never intended to be part of the inventory process. A discovery tool has been acquired and installation is complete. The final stage of documenting the policies and procedures for its use will be completed by June 30th, 2019.

Finding 2: Periodic Review of Access Privileges
Recommendation: We recommend that NWRDC management revise procedures to provide for comprehensive periodic reviews of access privileges to ensure that access privileges are authorized and appropriate. Such procedures should establish the method and frequency of reviews.

NWRDC Response: NWRDC agrees with this recommendation. The comprehensive review referenced in the report was completed in June, 2018. Finalization of the policies and procedures is underway to make this a regularly recurring process.

Finding 3: Appropriateness of Access Privileges
Recommendation: We recommend that NWRDC management ensure that assigned user access privileges promote an appropriate separation of duties.

NWRDC Response: NWRDC agrees with this recommendation. Due to the nature\use of the systems involved, the solitary permissions holder in question could not take actions that would result in personal gain. While we believe the risk for misuse to be small, we have reevaluated the employee's duties and the administrator privilege for the software in question has been removed.

Finding 4: Security Controls – Logical Access, User Authentication, and Configuration Management

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

NWRDC Response: NWRDC agrees with this recommendation. Steps have already been taken to resolve some of these issues. The remaining item will be corrected by June 30th, 2019.