STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-003
July 2017

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	Florida Atlantic University
Michael Barrett, Vice Chair and Management Committee Chair	Florida State University
David Cantrell, Non-Voting Member to February 23, 2017	Florida A&M University
Ronald Henry, Non-Voting Member from February 23, 2017	Florida A&M University
Michael Dieckmann	University of West Florida
Ted Duncan	Florida Department of Education
Levis Hughes, Management Committee Member	Florida Department of Education
Gene Kovacs	State University System of Florida Board of Governors

The team leader was Benjamin Ho, CISA, and the audit was supervised by Brenda Shiner, CISA.

Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

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. 2016-191. 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.

Finding 2: The NWRDC did not perform comprehensive periodic reviews of access privileges for the Windows server, Linux server, network, and mainframe environments.

Finding 3: NWRDC management needs to improve surplus storage media disposal documentation to better demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information.

Finding 4: Certain NWRDC security controls related to access, user authentication, configuration management, and logging and monitoring controls for NWRDC resources need improvement to ensure the confidentiality, integrity, and availability of NWRDC 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 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 action 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 NWDRC'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 periodic verification and inventory of IT resources housed and maintained at the NWRDC. Although NWRDC staff maintained various manually generated spreadsheets which contained information on the hardware and software assets within the data center and indicated that they had a tool that could be used to scan the NWRDC IT environment and generate a hardware and software asset listing of IT resources maintained and housed at the NWRDC, NWRDC staff had not performed a reconciliation of the spreadsheet information to hardware and software asset listings to ensure the various spreadsheets were complete and up-to-date. Also, our audit procedures disclosed that, as of February 7, 2017, a scan of the NWRDC IT environment had not been performed in over a year.

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.

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

Finding 2: Periodic Review of Access

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.

Our review disclosed that the *Manual* did not contain specific information regarding the method and frequency of required periodic reviews of access privileges. In response to our audit inquiry, NWRDC management stated that access reviews were performed on selected accounts; however, a

[1] NWRDC *Policy and Procedure Manual, Appendix E Information Security Program*, Effective Date: September 25, 2015.

comprehensive periodic review for all Windows server, Linux server, network, and mainframe environments was not performed.

Without procedures documenting the method and frequency of periodic reviews of all access privileges, management's assurance that access privileges were authorized and appropriate is limited.

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 the reviews.

Finding 3: Surplus Storage Media Disposal Documentation

Effective security controls include established procedures for the proper sanitization and disposal of storage media. Such procedures should address the safeguarding of storage media, including hard drives and data tapes, awaiting disposal to ensure accountability and control over the storage media and to protect any confidential and exempt information contained therein. To demonstrate that such procedures were followed, it is critical that organizations maintain complete and accurate disposal records to document that surplus storage media were sanitized, when and how the media were sanitized, and the final disposal process.

According to NWRDC management, the NWRDC sent 567 surplus hard drives (from equipment decommissioned on April 15, 2014) and 11 surplus data tapes to the University for recycling (i.e., disposal) on December 7, 2016. We reviewed the recycling documentation associated with the disposal and determined that, while the documentation noted the total number of items sent for recycling, NWRDC staff did not record for each of the items detailed information, such as the serial number of each hard drive and data tape disposed of, the serial number of the originating hardware associated with the items as applicable, the date of disposal, and the name of the person who sanitized each item. In response to our inquiry, NWRDC management stated that detailed information for each recycled item was not included on the documentation because the University did not require it for recycling the equipment. However, without detailed information, NWRDC cannot demonstrate that each of the hard drives and data tapes were sanitized and disposed of appropriately.

Without complete and accurate documentation of recycled storage media sanitization and disposal, management's ability to demonstrate that proper accountability and control of the storage media was maintained to prevent inappropriate or unauthorized access to confidential or exempt information is limited.

Recommendation: To improve documentation of storage media disposals and to demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information, we recommend that NWRDC management require that detailed documentation containing the serial numbers of both the disposed of storage media and the originating hardware, if applicable, the date of disposal, and the name of the person responsible for sanitization be maintained.

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

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 access controls, user authentication, configuration management, and logging and monitoring 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 have notified appropriate NWRDC management of the specific issues.

Without appropriate security controls related to access controls, user authentication, configuration management, and logging and monitoring the risk is increased that the confidentiality, integrity, and availability of customer entity data and related IT resources may be compromised.

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

PRIOR AUDIT FOLLOW-UP

The NWRDC had taken corrective actions for all findings included in our report No. 2016-191.

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 2016 through March 2017 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 2016 through March 2017 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; the safeguarding of IT resources; and the effectiveness and efficiency of IT operations.
- To determine whether management had corrected, or was in the process of correcting, deficiencies disclosed in our report No. 2016-191.

- 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 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 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 documentation to obtain an understanding of:
  - The organizational structure, key policies, procedures, and operational processes for the NWRDC.
  - The IT infrastructure and architecture of the NWRDC, including hardware, software, and operating systems for the various server platforms and network components.
- Evaluated the adequacy of NWRDC policies and procedures for IT resource inventory tracking and reconciliation.
- Evaluated the effectiveness of the NWRDC's software and IT infrastructure component change control process including hardware and system software changes, firewall changes, and software patch management. Specifically, we examined:
  - 25 of the 213 closed change requests made during the period July 1, 2016, through January 18, 2017, to determine whether the hardware and systems software changes were appropriately authorized, tested, and approved.
  - 10 of the 52 NWRDC physical and virtual Windows servers to evaluate whether, as of January 31, 2017, the NWRDC had timely installed vendor-supplied patches.

- 3 of the 16 NWRDC physical and virtual Linux servers to evaluate whether the NWRDC had timely installed vendor-supplied patches as of January 31, 2017.
- The mainframe production environment to evaluate whether the NWRDC installed vendor-supplied patches timely as of December 21, 2016.
- 8 selected network devices to evaluate whether the NWRDC installed vendor-supplied patches timely as of January 9, 2017.

- Evaluated the effectiveness of NWRDC logging and monitoring controls.
- Examined NWRDC's risk assessment plan and other related documentation and evaluated the effectiveness of the NWRDC's IT risk assessment process.
- Examined supporting documentation applicable to the storage and disposal of surplus hard drives and data tapes and evaluated the effectiveness of NWRDC processes and policies and procedures for storing and disposing of storage media.
- Evaluated the logical design, administration, and periodic review procedures for logical access privileges to NWRDC IT resources and customer entity data. Specifically, we reviewed:
  - The appropriateness of administrative access privileges for 1 of the 2 network domains used for NWRDC services and operations as of January 17, 2017.
  - The appropriateness of access privileges for 7 mainframe environment administrative accounts as of February 7, 2017.
  - The appropriateness of access privileges for 61 mainframe environment administrative accounts as of January 25, 2017.
  - The appropriateness of access privileges for 3 Linux servers as of February 16, 2017.

    The appropriateness of access privileges for 6 Windows servers as of February 16, 2017.
  - The appropriateness of access privileges for 8 network devices as of January 11, 2017 and January 24, 2017.
- Evaluated user authentication controls related to the NWRDC's IT infrastructure.
- 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 2, 2017

Higher Education Entities

Chipola College	Florida State University	Santa Fe College
Florida A&M University	Florida Virtual Campus	University of Central Florida
Florida Atlantic University	Miami Dade 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	Pensacola State College	University of West Florida
Florida State College of Jacksonville	Polk State College	

State 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 Okaloosa and Walton Counties	

K-12 School Districts

Alachua County District School Board	Leon 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
Hillsborough County District School Board	Suwannee County District School Board	Jefferson County District School Board
Lee 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 Jacksonville	LearnSomething, Inc.	Palm Beach County Clerk and Comptroller
Florida State University Foundation	Orange County Clerk of Courts	Tallahassee Memorial HealthCare, Inc.
Florida Surplus Lines Service Office	Orange County Board of County Commissioners	The Ringling Museum of Art, Florida State University
Health Care District of Palm Beach County	Palm Beach 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, Florida 32399-1450

June 30, 2017

Dear Ms. Norman,

Please accept Florida State University's response to your letter of May 31 with report of preliminary and tentative findings and recommendations from your recent audit of Northwest Regional Data Center. As always, please let us know if there are any questions or if we can be of 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 and CIO, Florida State University & Vice-Chair, NWRDC Policy Board
Mehran Basiratmand, CTO, Florida Atlantic University & Chair, NWRDC Policy Board

NWRDC Response

Finding 1: NWRDC management needs to improve policies and procedures to provide for the tracking and periodic 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 the IT resource inventory to asset listings and other applicable NWRDC records.

Response: NWRDC and FSU agrees with this recommendation. As part of the audit, NWRDC provided a complete inventory of the systems it owns and the systems it manages for its customers. For NWRDC systems, we have detailed the controls we have in place to keep servers\systems from being added without the proper authorization:

- All Unused network ports are turned off.
- All used network ports are locked to specific MAC addresses of the system, preventing an authorized system from being unplugged and an unauthorized system being plugged in.
- While customers may add systems to their networks, that does not place them under NWRDC control or responsibility. They must request that those be added to NWRDC's managed service, which adds the system to the customer inventory
- All authorized systems are inventoried manually.
- All network gear is inventoried manually.
- All physical equipment is inventoried manually.
- All capital equipment is additionally inventoried through FSU Equipment Accounting.
- All inventories are reviewed as part of the annual rate development process.

However, NWRDC does agree that we can and should do better in reconciling asset inventories and will take steps to improve.

Finding 2: The NWRDC did not perform comprehensive periodic reviews of access privileges for the Windows server, Linux server, network, and mainframe environments.

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 the reviews.

Response: NWRDC and FSU agrees with this recommendation. As part of the audit, NWRDC did provide evidence that routine checks are done on a periodic basis on sample sets of accounts. While not comprehensive, monitoring and reviews are performed.

Finding 3: NWRDC management needs to improve surplus storage media disposal documentation to better demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information.

> **Recommendation:** To improve documentation of storage media disposals and to demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information, we recommend that NWRDC management require that detailed documentation containing the serial numbers of both the disposed of storage media and the originating hardware, if applicable, the date of disposal, and the name of the person responsible for sanitization be maintained.
>
> **Response:** NWRDC and FSU agrees with this recommendation. As part of the audit, NWRDC did show that all FSU polices were followed in the disposal of surplus storage media. Additionally, FSU maintains a 3rd party contract to handle the destruction of all surplus storage media. While NWRDC did follow all policies and procedures, we agree we should go above and beyond the current requirements in documenting this process so that all parties can be reassured.

Finding 4: Certain NWRDC security controls related to access, user authentication, configuration management, and logging and monitoring controls for NWRDC resources need improvement to ensure the confidentiality, integrity, and availability of NWRDC customer entity data and related IT resources.

> **Recommendation:** We recommend that NWRDC management improve certain security controls related to access controls, user authentication, configuration management, and logging and monitoring to ensure the confidentiality, integrity, and availability of NWRDC customer entity data and related IT resources.
>
> **Response:** NWRDC and FSU agrees with this recommendation and will investigate ways to improve its existing controls and procedures in these areas.