STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2016-191
May 2016

FLORIDA STATE UNIVERSITY
NORTHWEST REGIONAL DATA CENTER

Data Center Operations

Sherrill F. Norman, CPA
Auditor General

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 NWRDC. The Board's primary function is to establish and promulgate policies for the NWRDC. The Executive Director, who is selected by the Board, is responsible for the overall administration of the NWRDC.

The Board members and customer entities represented and the Executive Director who served during the period of our audit were:

Board Member	Customer Entity Represented
Mehran Basiratmand, Chair	Florida Atlantic University
Michael Barrett, Vice Chair and Management Committee Chair	Florida State University
David Cantrell, Non-Voting Member	Florida A&M University
Michael Dieckmann	University of West Florida
Ted Duncan	Department of Education
Levis Hughes, Management Committee Member	Department of Education
Gene Kovacs	State University System of Florida Board of Governors
Damu Kuttikrishnan	Department of Revenue
Henry Martin, Management Committee Member	Walton County District School Board
Peter M. Taylor, Board Member Emeritus and Non-Voting Member	Florida International University

Tim Brown, Executive Director

The team leader was Milli Aschauer 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:

www.myflorida.com/audgen

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. 2015-101. Our audit disclosed the following:

Finding 1: Change management controls related to hardware and systems software changes need improvement to ensure that only authorized, tested, and approved hardware and systems software changes are implemented into the production environment. Similar findings were noted in our report No. 2015-101.

Finding 2: The NWRDC had not developed a written, comprehensive IT risk assessment plan to provide a documented basis for managing IT-related risks.

Finding 3: The NWRDC needs to improve surplus computer hard drive sanitization and disposition 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 user authentication and physical security for NWRDC IT resources need improvement to ensure the confidentiality and availability of NWRDC customer entity data and related IT resources. A similar finding related to user authentication was communicated to NWRDC management in connection with prior audits of the NWRDC, most recently in connection with our report No. 2015-101.

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 selects an Executive Director to be 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 employees of the University and are to follow University policies for payroll, leave, and other personnel actions.

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. Lists of the

NWRDC customer entities and services offered by the NWRDC are included in this report as ***EXHIBIT A*** and ***EXHIBIT B***, respectively.

FINDINGS AND RECOMMENDATIONS

Finding 1: Change Management Controls

Effective change management controls over modifications to hardware and systems software ensure that only authorized, tested, and approved changes are implemented into the production environment. Such controls include written procedures addressing the detailed requirements for documenting and tracking the testing and implementation of hardware and systems software changes. Further, the effectiveness of change management controls is enhanced through controls that ensure that the change management control process is followed when changes are implemented into the production environment.

Our audit procedures disclosed that some NWRDC change management controls related to hardware and systems software changes need improvement. Specifically, we found that:

- The NWRDC had not established detailed written procedures related to the tracking, documenting, and approval of hardware and systems software changes.
- Although the NWRDC used a change management system for tracking the authorization, testing, and implementation of hardware and systems software changes, the NWRDC had not established controls, such as the use of a reconciliation process or other controls, to ensure that all changes implemented into the production environment followed the change control process.
- The NWRDC did not always maintain documentation supporting that hardware and systems software changes were appropriately tested and functioned as intended prior to being implemented into the production environment. Specifically, we noted that for two of three hardware and systems software changes implemented between July 15, 2015, and August 20, 2015, the NWRDC could not provide documentation that the changes were tested and functioned as intended prior to their implementation into the production environment.
- The NWRDC did not maintain documentation supporting that hardware and systems software changes were approved prior to their implementation into the production environment.

Similar findings were noted in prior audits of the NWRDC, most recently in our report No. 2015-101. In response to our audit inquiry, NWRDC management stated that appropriate change management controls to address the issues noted above are being implemented with a projected completion date of June 30, 2016.

Absent effective change management controls to ensure that all hardware and systems software changes are authorized, tested, and approved, the risk is increased that erroneous or unauthorized hardware or systems software changes may be implemented into the production environment and not be timely detected.

Recommendation: NWRDC management should continue implementation of change management controls to ensure that only authorized, tested, and approved hardware and systems software changes are implemented into the production environment.

Finding 2: IT Risk Assessment

Management of IT-related risks is a key part of enterprise IT governance. Incorporating an enterprise perspective into day-to-day governance actions helps entity personnel understand the entity's greatest security risk exposures and determine whether planned controls are appropriate and adequate to secure IT resources from unauthorized disclosure, modification, or destruction. A comprehensive, written IT risk assessment, including the identification of risks and the evaluation of the likelihood of threats and the severity of threat impact, assists management in establishing cost-effective measures to mitigate risks and, where appropriate, formally accept residual risks. University policy[1] provides that all University units and related affiliate organizations are responsible for conducting and monitoring risk assessments to ensure that any potential threats to their physical areas and information systems are identified and evaluated.

Our audit procedures disclosed that the NWRDC had not developed a comprehensive, written IT risk assessment to identify risks and evaluate the likelihood of threats and the severity of threat impact to the data center and related IT resources. However, our examination of documentation provided by NWRDC management disclosed that the NWRDC was in the process of developing an IT risk assessment plan that will include the completion of an initial IT risk assessment during the 2016-17 fiscal year.

The absence of a comprehensive, written IT risk assessment may lessen the NWRDC's assurance that risks and all likely threats and vulnerabilities have been identified and evaluated, the most significant risks have been addressed, and appropriate decisions have been made regarding which risks to mitigate through appropriate security controls, and which residual risks to formally accept.

Recommendation: We recommend that NWRDC management continue the development of a comprehensive, written IT risk assessment plan to provide a documented basis for managing IT-related risks.

Finding 3: Surplus Computer Hard Drive Sanitization and Disposition Documentation

Effective security controls include established procedures for the proper sanitization and disposal of storage media. Such procedures should address the safeguarding of surplus computer hard drives awaiting disposal to ensure accountability and control over the hard drives 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 computer hard drives were sanitized, when and how they were sanitized, and the final disposition.

University policy[2] requires that all surplus computers be sanitized prior to their release to surplus for disposal. A completed sanitization sticker must be attached to the surplus computer hard drive that includes information indicating the date the surplus computer hard drive was sanitized and the name of the person who sanitized it. In addition to the sanitization sticker, a *Property Accountability Release Form*

[1] Florida State University Policy 4-OP-F-7 *POLICY ON SAFEGUARDING OF CONFIDENTIAL FINANCIAL AND PERSONAL INFORMATION*, Effective Date: January 1, 2014.

[2] Florida State University Policy 4-OP-D-2-F *PROPERTY*, Effective Date: January 1, 2014.

(*PAR Form*) must be completed for each surplus computer documenting serial numbers, the initials of the person who sanitized the surplus computer hard drive, and the disposition method.

On October 23, 2015, as part of our audit, we examined 5 of the 10 hard drives removed from surplus computers. Our examination disclosed that NWRDC staff appropriately sanitized the hard drives and placed a sanitization sticker on each of the removed hard drives indicating the date the hard drive was sanitized and the name of the person who sanitized the hard drive. However, NWRDC staff did not complete the *PAR Forms* in accordance with University policy or otherwise maintain documentation that associated the removed hard drives with the originating surplus computers. Specifically, our review of all *PAR Forms* completed by NWRDC staff during the period February 3, 2015, through November 4, 2015, disclosed that, contrary to University policy, a single form was used for multiple surplus computer hard drives and did not contain identifying information (e.g., serial numbers) of either the surplus computers or the removed hard drives or the initials of the person who performed the sanitization. Therefore, we were unable to determine that all hard drives associated with the surplus computers were appropriately removed and sanitized.

Without accurate and complete documentation of surplus computer hard drive sanitization and disposition, management's ability to demonstrate that appropriate accountability and control of hard drives has been maintained to prevent inappropriate or unauthorized access to confidential or exempt information is limited.

Recommendation: To improve documentation of surplus computer hard drive sanitization and disposition and demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information, we recommend that NWRDC management ensure that *PAR Forms* are completed in accordance with University policy.

Finding 4: Security Controls – User Authentication and Physical Security

Security controls are intended to protect the confidentiality, integrity, and availability of data and related IT resources. Our audit procedures disclosed that certain security controls related to user authentication and physical security 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 user authentication and physical security, the risk is increased that the confidentiality, integrity, and availability of data and related IT resources may be compromised. A similar finding related to user authentication was communicated to NWRDC management in connection with prior audits of the NWRDC, most recently in connection with our report No. 2015-101.

Recommendation: We recommend that NWRDC management improve certain security controls related to user authentication and physical security 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. 2015-101.

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 October 2015 through December 2015 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 NWRDC during the period July 2015 through December 2015 and selected actions in February 2015, and through February 10, 2016. 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.
- To determine whether management had corrected, or is in the process of correcting, deficiencies disclosed in our report No. 2015-101.
- 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 the 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.
- Obtained an understanding of the NWRDC's governance, organizational structure, key policies, procedures, and operational processes.
- Evaluated the NWRDC's compliance with selected statutory and contractual requirements. Specifically, we reviewed:
    - The Policy Board membership established for the 2015-16 fiscal year to evaluate compliance with Section 1004.649(1)(a), Florida Statutes.
    - Service level agreements (i.e., contracts) with NWRDC customers to evaluate compliance with Section 1004.649(1)(c), Florida Statutes, as well as the monitoring and reporting of service level agreement metrics to determine whether contractual requirements were met.
    - Six customer service tickets created between October 1, 2015, and October 13, 2015, to determine whether NWRDC response times were within contractually agreed upon response time requirements.
- Obtained an understanding of the NWRDC's computing environment including its IT infrastructure and architecture.
- Obtained an understanding of the services provided and offered by the NWRDC for the 2015-16 fiscal year.
- Obtained an understanding and evaluated the NWRDC's risk assessment process.
- Obtained an understanding and evaluated the effectiveness of controls applicable to the NWRDC's vulnerability testing of its networks and hosted systems.
- Obtained an understanding and evaluated the effectiveness of the NWRDC's processes and policies and procedures, including supporting documentation, applicable to the storage, sanitization, and disposition of surplus computers, hard drives, and data tapes.
- Evaluated physical access controls to selected areas of the NWRDC as of October 26, 2015.
- Examined on October 23, 2015, 5 of 10 hard drives removed from surplus computers and sanitized by NWRDC staff to determine whether the hard drives had been appropriately sanitized.
- Obtained an understanding and evaluated the effectiveness of the NWRDC's logical access controls for its network components and systems software. Specifically, we evaluated:
    - The effectiveness of user authentication controls for network components as of November 6, 2015, and mainframe system network components as of November 24, 2015, and December 17, 2015.
    - The appropriateness of access privileges of all 41 system administrator accounts of selected NWRDC systems software computing environments as of November 9, 2015, November 24, 2015, and December 17, 2015.

- The appropriateness of access privileges of all 10 network administrator accounts as of November 4, 2015, and November 9, 2015, based on the type of network computing environment.

- Obtained an understanding and evaluated the effectiveness of backup controls in place to ensure the continuity of data center operations, including appropriate tape backup, tape rotation, and provisions for off-site backup storage locations. Specifically, we evaluated:
  - The appropriateness of backup processes and procedures used by the NWRDC, including the appropriateness of the NWRDC's off-site backup storage locations.
  - The appropriateness of physical access privileges for 16 individuals with access to backup tapes stored at an off-site backup storage location as of October 19, 2015.
- Reviewed and evaluated the inventory records of 246 backup tapes stored at an off-site backup storage location on November 5, 2015, and verified the existence of 25 of the 246 backup tapes listed on the inventory records and located at the off-site backup storage location.
- Obtained an understanding and evaluated the effectiveness of capacity planning and performance monitoring.
- Obtained an understanding and evaluated the effectiveness of the NWRDC's change management controls in place during the period July 1, 2015, through February 10, 2016, to determine whether the NWRDC had performed appropriate procedures to determine whether hardware and systems software changes were appropriately authorized, tested, functioned as intended, approved, and subsequently implemented into the production environment by appropriate individuals.
- 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

LIST OF NWRDC CUSTOMER ENTITIES

AS OF FEBRUARY 10, 2016

Higher Education

Chipola College	New College of Florida
Florida A&M University	Pensacola State College
Florida Atlantic University	Polk State College
Florida Gulf Coast University	St. Thomas University
Florida International University	University of Central Florida
Florida State College of Jacksonville	University of Florida
Florida State University	University of North Florida
Florida State University Foundation	University of South Florida
Florida Virtual Campus	University of West Florida

State Government

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

K-12 School Districts

A.D. Henderson University School	Santa Rosa County District School Board
Bay County District School Board	St. Johns County District School Board
Escambia County District School Board	Suwannee County District School Board
Florida State University Developmental Research School	
Hillsborough County District School Board	
Lee County District School Board	
Nassau County District School Board	
Palm Beach County District School Board	

Panhandle Area Educational Consortium:

Calhoun County District School Board	Liberty County District School Board
Franklin County District School Board	Madison County District School Board
Gadsden County District School Board	Taylor County District School Board
Gulf County District School Board	Wakulla County District School Board
Holmes Beach County District School Board	Walton County District School Board
Jackson County District School Board	Washington County District School Board
Jefferson County District School Board	

Local Government, Health Care, and Other

City of Jacksonville	Orange County Clerk of Courts
City of Tallahassee	Palm Beach County Board of County Commissioners
Florida Surplus Lines Service Office	Palm Beach County Clerk and Comptroller
Health Care District of Palm Beach County	Tallahassee Memorial HealthCare, Inc.
LearnSomething, Inc.	The Ringling Museum of Art, Florida State University
Orange County Board of County Commissioners	

EXHIBIT B

LIST OF SERVICES OFFERED BY THE NWRDC

AS OF FEBRUARY 10, 2016

Service Category	Service Description
Facilities Services	Raised Floor Space
	Electrical Circuits (Surcharge and Installation)
	Collocation Support and Monitoring
	Off-site Collocation
Infrastructure Services	Cloud Infrastructure Service
	Standard Physical Server (3 Options)
	Custom Physical Server Configurations
Storage and Recovery Services	Backup
	Tier 1 Storage
	Tier 2 Storage
	Tier 3 Storage
	Modular Storage
	Remote Replication
	Internal Replication
	Fiber Channel Ports
	IOPS On Demand
Network Services	Network 10GB Fiber Port
	Network 1GB Port
	Commodity Internet Access
	Network VPN Tunnel
	VPN Client
	Tallahassee Fiber Loop Right to Use
	Tallahassee Fiber Loop Maintenance
Managed Services	System Administrator (Server)
	System Administrator (Virtual Host)
	Patch Management Toolset
	Infrastructure Monitoring Toolset
	Personnel
	Backup Administrator
	Storage Administrator
	Network Administrator
	Operator
	System Administrator
Security Services	Penetration Test
Mainframe Services	Mainframe Processing

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
May 3, 2016

Dear Ms. Norman,

Please accept Florida State University's response to your April 4th 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

Finding 1: Change management controls related to hardware and systems software changes need improvement to ensure that only authorized, tested, and approved hardware and systems software changes are implemented into the production environment. Similar findings were noted in our report No. 2015-101.

> **Response:** NWRDC agrees with this finding and that improvements should be made to its change management process. NWRDC updated its change management policy on Oct. 27th, 2015. NWRDC will continue developing the reconciliation process to be implemented June 30th, 2016.

Finding 2: The NWRDC had not developed a written, comprehensive IT risk assessment plan to provide a documented basis for managing IT-related risks.

> **Response:** NWRDC agrees with this finding. While NWRDC has been performing risk assessments, we agree that improvements should be made. As discussed, efforts are already underway to develop a new risk assessment process, which will be implemented in FY16-17.

Finding 3: The NWRDC needs to improve surplus computer hard drive sanitization and disposition documentation to better demonstrate that appropriate actions were taken to prevent inappropriate or unauthorized access to confidential or exempt information.

> **Response:** NWRDC agrees with this finding and has already taken steps to improve this process.

Finding 4: Certain NWRDC security controls related to user authentication and physical security for NWRDC IT resources need improvement to ensure the confidentiality and availability of NWRDC customer entity data and related IT resources. A similar finding related to user authentication was communicated to NWRDC management in connection with prior audits of the NWRDC, most recently in connection with our report No. 2015-101.

> **Response:** NWRDC agrees with this finding.