OFFICE OF INDEPENDENT INTERNAL AUDIT

Audit of DeKalb County Data Center Physical Security

Audit Report No. 2018-007-IT
August 2019

DEKALB COUNTY GOVERNMENT

Department of Innovation & Technology

FINAL REPORT

John L. Greene, CIA,CIG,CGAP,CGFM
Chief Audit Executive

Page intentionally left blank

DeKalb County GEORGIA

John Greene
Chief Audit Executive

AUDIT OF DEKALB COUNTY DATA CENTER PHYSICAL SECURITY
AUDIT REPORT NO. 2018-007-IT

FINAL REPORT

What We Did

In accordance with the Office of Independent Internal Audit's (OIIA) Annual Audit Plan, we conducted a performance audit of the DeKalb County Data Center Physical Security. The objective of this audit was to assess the effectiveness of the physical security procedures related to the County's data centers. This audit will be performed as part of the OIIA's mission to provide independent, objective, insightful, nonpartisan assessment of stewardship or performance of policies, programs and operations in promoting efficiency, effectiveness and integrity in DeKalb County. The audit focused on the data centers where the County computer systems are housed.

What We Found

We identified a number of areas that require improvements related to the physical security of the County's data centers. Many of these findings are confidential and are not disclosed in detail because disclosing their content would put the County at further risk. The information about the confidential findings noted in this report only provides summary level information in order to protect the County's data center operations. The audit identified 17 recommendations to address the findings noted. Specific and detailed findings along with recommendations were discussed with the Department of Innovation and Technology (DoIT).

What We Recommend

We recommend that management develop and implement additional processes and procedures to ensure threats to the data centers are addressed and the major areas of risk have either been resolved or that mitigating controls have been put in place. Some of the general recommendations included developing a memorandum of understanding regarding physical security requirements with other parties sharing data center responsibilities; strengthening safeguards to mitigate the risks associated with environmental controls and data center infrastructure including equipment maintenance; coordinating and enhancing disaster recovery efforts; improving access management procedures; and implementing monitoring procedures to identify, report, and resolve issues of noncompliance.

What Management Responded

The DeKalb County DoIT appreciates the hard work and diligence that went into this Data Center Physical Security audit, and looks forward to implementing appropriate changes and enhancements to processes and procedures as recommended. It is important to note that many of the findings are outside of DoIT's management control, however, we will be coordinating with appropriate departments/agencies to facilitate process and/or procedural changes to enhance the county's overall data center physical security stance, and will enable the county to move all of the control objective conclusions to that of a Best Practice.

DoIT concurs with each of the recommendations cited, and has already implemented a number of changes based on our initial review of the audit findings/recommendations. DoIT will address each of the findings as the process allows for, but in general, we have already addressed some of the issues noted related to Facilities signage and access management associated with other department/agency staff that share (or believe they share) data center responsibilities. DoIT will aggressively implement additional safeguards for those areas that are under DoIT sole control, and will coordinate with other departments/agencies as appropriate to facilitate additional enhancements related to environmental controls, data center infrastructure, and access control - which is currently outside of DoIT auspices - as this is jointly managed by three other county departments/agencies (Facilities Management, Police Department and Sheriff Office). Though DoIT has implemented and maintains monitoring procedures to help identify issues of noncompliance, we appreciate the recommendations that will help strengthen the county's data centers overall physical security. The Department of Innovation and Technology will continue to work with the Office of Independent Internal Audit, the Administration and the Governing Authority to make reasonable changes, keeping in mind that some of the changes and enhancements may take longer depending on other departments/agencies willingness to conform to best practices. In some cases the county may decide to defer implementing a recommendation if an associated risk assessment identifies that though something may be a best practice, other mitigating controls are in place to maintain appropriate levels of data center security.

Summary of conclusions:

Control Objective	Initial	Notable	Adequate	Best Practice
1. Data Center Policies and Procedures	[redacted]			
2. Data center server inventory control				
3. Site Location*				
4. Site Perimeter Surveillance*				
5. Physical Security*				
6. Access Management*				
7. Computer Room Location and Infrastructure*				
8. Environmental Security*				
9. Environmental Equipment Maintenance*				
10. Security Awareness Training				
11. Disaster Recovery Plan				
12. Data Backup				

* The facilities where these data centers are located are managed by [redacted]

Table of Contents

BACKGROUND AND INTRODUCTION ---- 6
AUDIT RESULTS ---- 7
FINDING 1 – Data Center Usage Policy/Agreement ---- 7
FINDING 2 – Physical Security Policies and Procedures - Confidential ---- 8
FINDING 3 – Data Center Site Inspection Enforcement - Confidential ---- 8
FINDING 4 – Data Center Server Inventory ---- 8
FINDING 5 – Signs: No Restricted Access and Prohibiting Food and Drink ---- 8
FINDING 6 – Unlocked Cabinet ---- 9
FINDING 7 – Environmental Security Needs Improvement - Confidential ---- 10
FINDING 8 – Physical Access to the Data Centers - Confidential ---- 10
FINDING 9 – Access Management - Confidential ---- 10
FINDING 10 – Environmental and Safety Monitoring/Temperature Control - Confidential ---- 10
FINDING 11 – Data Center Combustible Materials - Confidential ---- 10
FINDING 12 – Fire Suppression - Confidential ---- 10
FINDING 13 – Disaster Recovery (DR) - Confidential ---- 11
FINDING 14 – Data Backup - Confidential ---- 11
FINDING 15 – Data Backup Software - Confidential ---- 11
FINDING 16 – Security Awareness Training ---- 11
FINDING 17 – Physical Security Policy/Non-Disclosure Agreement (NDA) ---- 12
APPENDIX ---- 13
Appendix I – Purpose, Scope and Methodology ---- 13
Appendix II – Definitions and Abbreviations ---- 14
DISTRIBUTION ---- 15
PROJECT TEAM ---- 16
STATEMENT OF ACCORDANCE ---- 17

BACKGROUND AND INTRODUCTION

Every program or service that DeKalb County provides involves information technology. The use of information technology results in data and information that must be secured in order to maintain the data's confidentiality, integrity, and availability. Data confidentiality refers to the appropriate controls in place to ensure authorization and authentication of all users before access is granted, based on job-level responsibilities and the principle of least-privilege access. Data integrity refers to the controls that ensure the accuracy and consistency of the system generated results. Data availability refers to the controls that ensure the ability to access data when needed, and, most importantly, to minimize or eliminate system downtime, business disruption, or a disaster event, all of which could lead to lost productivity and service interruptions to citizens and County personnel.

A data center is used to house network server systems and associated components. This facility is dedicated to securing data and systems. One of the most important responsibility areas for data centers is physical security. Despite the move to cloud-based infrastructure, data centers are still a critical physical fortress protecting critical data from physical exposure. The data centers listed below are County owned and operated facilities used to house the critical telecommunications, data, and computing resources, including individually operating domains, applications, and databases, which support the Police, Fire and Rescue, Superior Court, State Court, Sheriff, Tax Commissioner, Budget Office, Finance, Human Resources, Property Appraisal, Purchasing & Contracting, Innovation & Technologies and all County's agencies and elected officials.

There are three separate data center locations serving the County;

- [redacted]
- [redacted], and
- [redacted]

The DeKalb County Department of Innovation and Technology (DoIT) is responsible for providing technology vision and leadership, as well as day-to-day information technology support, for all facets of DeKalb County government. In addition, DoIT supports applications, networking and telecommunications, servers, and security provisioning at [redacted] data center. However, the Police Division Advanced Technology Unit (ATU) provides application support for the computing resources in the data center located at the [redacted].

The County has its own wide area network (WAN), [redacted]
County's data centers must provide internal and external users with the capacity for data confidentiality, integrity, and availability.

The County's Physical Security policy dated January 1, 2014, states the intent of the policy is to help employees determine what physical locations can be accessed by employees and with what level(s) of authorization. In addition, it states that physical security access means either having actual access at all times or requesting temporary access to a restricted area. The policy states

that the guidelines include, but are not limited to, data centers, data suites and closets or any room where servers and switching equipment may be housed throughout the County and under the jurisdiction of the DoIT. This policy was used during the audit to complete our assessment of physical security processes and controls.

AUDIT RESULTS

The audit concluded that while many internal controls are in place over the physical security of the County's data centers, several areas require improvement related to the physical security of the data center operations. DoIT is held primarily responsible for the management and physical security of the data centers. However, they do not have sole authority over these areas. We noted that this presents challenges in ensuring physical security. We noted instances of noncompliance with DoIT policies and procedures. We also noted that DoIT has limited authority to enforce the physical security control objectives they have developed. A key component to improving the physical security controls will be developing and implementing an agreement regarding governance of data center operations. In addition, obtaining support from County senior management to enforce such agreement and the physical security policies and procedures will be critical.

FINDING 1 – Data Center Usage Policy/Agreement

Objective: Assess the effectiveness of the physical security procedures related to the County's data centers.

Criteria: Benchmarking and audit research noted written usage agreements in environments where data centers were either outsourced to a third party or located in areas outside of direct Information Technology management and control.

Condition: There is no formal usage agreement governing the County data center locations. Facilities management, Sheriff, Police, and others have some authority and control over the facilities where data centers are located. However, the Department of Innovation & Technology is ultimately responsible for the management and physical security of the data centers.

Cause: Although Innovation and Technology have some policies and procedures related to the data center operations, there is no requirement for other County management areas such as Facilities, Sheriff, and Police to comply with those policies and procedures.

Consequence: Without such agreement, the Department of Innovation and Technology may find it difficult to ensure physical security of the data center locations because their management and control includes other areas outside of Innovation and Technology.

Recommendation: We recommend that management develop and implement formal agreement regarding governance activities and requirements related to the data centers.

FINDING 2 – Physical Security Policies and Procedures - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 3 – Data Center Site Inspection Enforcement - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 4 – Data Center Server Inventory

Objective: Assess the effectiveness of the physical security procedures related to the County's data centers.

Criteria: Per National Institute of Standards and Technology (NIST), the organization should develop and documents an inventory of information system components that accurately reflects the current information system, includes all components within the authorization boundary of the information system, the inventory should be at the level of granularity deemed necessary for tracking, reporting, reviewing, and updating the information system component inventory.

Condition: At the time of the audit, the data center server inventory was incomplete. We received inventory records with missing serial numbers, IP addresses, model numbers, and server functions. However, management indicated that they use multiple tools to obtain and document server inventory. Therefore, the missing information can be obtained elsewhere.

Cause: The lack of resources to acquire more current methodology to document and maintain inventory could be impacting this recognized standard.

Consequence: Weak controls over asset inventory create an environment where information technology assets become vulnerable to loss, theft, or exposure. The risk of loss, theft, or the inadvertent release of sensitive information can decrease the public's confidence in the County's ability to monitor and use its resources securely.

Recommendation: We recommend that management develop action plans to improve the controls related to asset management to ensure that all information assets are documented and changes are updated timely.

FINDING 5 – Signs: No Restricted Access and Prohibiting Food and Drink

Objective: Assess the effectiveness of the physical security procedures related to the County's data centers.

Criteria: The Physical Security Policy states that restrictive areas will be marked as "Restricted Area, DoITS Access Only." In addition, the policy states that these areas must display on the door of a restricted area, "Contact Security for access".

Condition: During the walkthrough phase of this audit, several situations related to the physical environment inside the data centers were noted.

- No restricted access signs (both locations).
- No signs prohibiting food and drink were evident outside or inside the computer room (both locations). A microwave and coffee maker were located inside one of the centers.
- At one of the data centers, there is a sign on the wall opposite from the security officer's desk that shows the direction to the data center.

Cause: Distributed management of the data center locations impacts enforcement of some policies and procedures.

Consequence: The lack of adherence to policies and procedures increases the risk that the security of the technology environment will be compromised. Such compromise could result in loss of data, interruption of services and operational difficulties.

Recommendation: We recommend that management develop and implement appropriate signs for the data center locations.

FINDING 6 – Unlocked Cabinet

Objective: Assess the effectiveness of the physical security procedures related to the County's data centers.

Criteria: According to the National Institute of Standards and Technology (NIST), the organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.

Condition: During our walkthrough, we noted a server rack was unlocked and the door left open.

Cause: The distributed responsibility for the data center locations may make it difficult to ensure the effectiveness of controls.

Consequence: Unsecured servers could result in exposing the network equipment to theft, damage, or tampering.

Recommendation: We recommend that management:

- Develop a procedure regarding how data center equipment should be secured. These procedures should include security for server racks.
- Periodically monitor the server environments at the data center to ensure equipment are protected.

FINDING 7 – Environmental Security Needs Improvement - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 8 – Physical Access to the Data Centers - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 9 – Access Management - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 10 – Environmental and Safety Monitoring/Temperature Control - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 11 – Data Center Combustible Materials - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 12 – Fire Suppression - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 13 – Disaster Recovery (DR) - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 14 – Data Backup - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 15 – Data Backup Software - Confidential

Note: The details of this finding are confidential under the exemptions noted in Georgia Open Records Act #50-18-70. The details of this finding would put the organization at risk. For questions and further information should be requested from the Chief Audit Executive of the Office of Independent Internal Audit.

FINDING 16 – Security Awareness Training

Objective: Assess the effectiveness of the physical security procedures related to the County's data centers.

Criteria: According to the National Institute of Standards and Technology (NIST), a robust and enterprise wide awareness and training program is paramount to ensuring that people understand their IT security responsibilities, organizational policies, and how to properly use and protect the IT resources entrusted to them.

Condition: The Department of Innovation & Technology has various training and awareness activities that included components of IT security, for example Georgia Crime Information Center (GCIC) Security Awareness training course. However, the audit found that these activities were not mandatory or scheduled on a periodic basis, nor is it clear whether these activities provide comprehensive coverage of key IT security responsibilities and there was no evidence that training has been completed by all employees.

Cause: Informal training occurs as employees perform their job. In addition, there is a lack of resources to focus on training and training documentation on a regular basis.

Consequence: A lack of training may result in staff not understanding the controls appropriate for the computer room. This may result in accidental or malicious damage to the County's equipment resulting in loss of data, interruption of IT services and operational difficulties.

Recommendation: We recommend that management establish a formal security awareness training program that includes details of the policies and procedures staff must follow, guidance on escalation and roles and responsibilities. Evidence of a formal training record should be maintained.

FINDING 17 – Physical Security Policy/Non-Disclosure Agreement (NDA)

Objective: Assess the effectiveness of the physical security procedures related to the County's data centers.

Criteria: The institution should protect the confidentiality of customer and institution information. A non-disclosure agreement can be used to put all parties on notice that the institution owns its information, expects strict confidentiality, and prohibits information sharing outside of that required for legitimate business needs.

Condition: Persons who have access to the data centers are not required to sign a physical security policy and non-disclosure agreement.

Cause: General policy exists informing employees regarding the need to secure certain information.

Consequence: A breach in confidentiality could disclose proprietary information, increase fraud risk, damage the County's reputation, violate customer privacy and associated rights, and violate laws or regulations.

Recommendation: We recommend that management obtain signed Physical Security Policy and non-disclosure agreement before granting employees and contractors access to computer systems.

APPENDIX

Appendix I – Purpose, Scope and Methodology

Purpose

The purpose of the engagement was to assess the effectiveness of the physical security procedures related to the County's data centers.

Scope and Methodology:

The scope of the audit focused on the locations where County computer systems are housed.

[redacted]

The methodology included control objectives and audit guidelines outlined in the Control Objectives for the Information and Related Technology (COBiT), issued by the Information Systems Audit and Control Association, guidelines issued by the National Institute of Standards and Technology (NIST), and County policies and best practices. Also, it included the following activities:

- Research related best practices.
- Review County physical security policies and procedures with Innovation and Technology management.
- Observe the operations at the data center locations.
- Interview appropriate County personnel.
- Review any other applicable documentation and information.

Appendix III – Definitions and Abbreviations

Acronyms and Abbreviation

CEO	Chief Executive Officer
NIST	The National Institute of Standards and Technology
COBiT	Control Objectives for the Information and Related Technology
DoIT	DeKalb County Department of Innovation and Technology
CIO	Chief Information Officer
CISO	Chief Information Security Officer
ATU	Advanced Technology Unit
GCIC	Georgia Crime Information Center

Key Definitions

WAN: A WAN (wide area network) is a communications network that spans a large geographic area such as across cities, states, or countries. They can be private to connect parts of a business or they can be more public to connect smaller networks together.[1]

1 What Is a Wide Area Network (WAN)? Lifewire. Retrieved 07/16/2019

DISTRIBUTION

Action Official Distribution:

John Matelski, CIO, Director of Innovation & Technology Department

Barry Puckett, Deputy Director of Infrastructure, Innovation & Technology Department

Vernon Greene, CISO, IT Security Manager, Innovation & Technology Department

Statutory Distribution:

Michael L. Thurmond, Chief Executive Officer

Nancy Jester, Board of Commissioners District 1

Jeff Rader, Board of Commissioners District 2

Larry Johnson, Board of Commissioners District 3

Steve Bradshaw, Board of Commissioners District 4

Mereda Davis Johnson, Board of Commissioners District 5

Kathie Gannon, Board of Commissioners District 6

Lorraine Cochran-Johnson, Board of Commissioners District 7

Harold Smith, Chairperson, Audit Oversight Committee

Harmel Codi, Vice Chairperson, Audit Oversight Committee

Adrienne T. McMillion, Audit & Oversight Committee

Claire Cousins, Audit & Oversight Committee

Gena Major, Audit Oversight Committee

Information Distribution:

Zachary L. Williams, Chief Operating Officer/ Executive Assistant

Vivian Ernstes, County Attorney

La'Keitha D. Carlos, CEO's Chief of Staff

Antwyn Brown, Chief of Staff, Board of Commissioners

Stacey Kalberman, Ethics Officer, DeKalb Board of Ethics

PROJECT TEAM

This report was submitted by:

Jin Veeranarong — August 13, 2019

Jin Veeranarong, CISA, CRISC
IT Auditor, Principal
Office of Independent Internal Audit

Date

This report was reviewed by:

Yolanda Lockett — August 13, 2019

Yolanda Lockett, CIA, CISA
IT Audit Manager
Office of Independent Internal Audit

Date

The report was approved by:

August 13, 2019

John Greene, CIA,CIG,CGAP,CGFM
Chief Audit Executive
Office of Independent Internal Audit

Date

STATEMENT OF ACCORDANCE

Statement of Accordance

The mission of DeKalb County is to make the priorities of the citizens of DeKalb County; the priorities of County government - by achieving a safer DeKalb, building stronger neighborhoods, creating a fiscally accountable and more efficient county government and uniting the citizens of DeKalb County.

The mission of the Office of Independent Internal Audit is to provide independent, objective, insightful, nonpartisan assessment of the stewardship or performance of policies, programs and operations in promoting efficiency, effectiveness and integrity in DeKalb County.

This performance audit was prepared pursuant to DeKalb County, Georgia – Code Ordinances/Organizational Act Section10A- Independent Internal Audit. We conducted this performance audit 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 our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

This report is intended for the use of the agency to which it was disseminated and may contain information that is exempt from disclosure under applicable law. Do not release without prior coordination with the Office of Independent Internal Audit.

Please address inquiries regarding this report to the Office of Independent Internal Audit at 404-371-2765.