

DURHAM



1869  
CITY OF MEDICINE

**TECHNOLOGY SOLUTIONS ACCESS CONTROL  
PERFORMANCE AUDIT**

**AUGUST 2012**

DURHAM



1869  
CITY OF MEDICINE

**CITY OF DURHAM**  
AUDIT SERVICES DEPARTMENT

*“Provides independent, objective  
assurance and investigative services”*

***Director of Audit Services***

Germaine Brewington, MBA, CPA, CFE

***Assistant Director of Audit Services***

Sonal Patel, CPA, CIA

***Senior Internal Auditor***

Craig Umstead, CFE, CFSA

***Internal Auditor***

Alex Terry, MPA

***Audit Assistant***

Asha Guta

**FRAUD, WASTE & ABUSE HOTLINE | 919.560.4213, EXT. 3**

**[WWW.DURHAMNC.GOV/DEPARTMENTS/AUDIT](http://WWW.DURHAMNC.GOV/DEPARTMENTS/AUDIT)**

DURHAM



1869  
CITY OF MEDICINE

**CITY OF DURHAM**

*Audit Services Department*

101 CITY HALL PLAZA | DURHAM, NC 27701

919.560.4213 | F 919.560.1007

[www.DurhamNC.gov](http://www.DurhamNC.gov)

**To:** Audit Services Oversight Committee  
**From:** Germaine Brewington, Director  
Audit Services Department  
**Date:** August 3, 2012  
**Re:** Transmittal: Technology Solutions Access Controls  
Performance Audit (August 2012)

The Department of Audit Services completed the report on the Technology Solutions Access Controls Performance Audit dated August 2012. The purpose of the audit was to determine the adequacy of User Access Controls at the Department of Technology Solutions and verify that employees of the Technology Solutions department have access consistent with their job responsibilities.

This report presents the observations, results, and recommendations of the Technology Solutions Access Controls Performance Audit dated August 2012. City management concurs with the recommendations made. Management's response to the recommendations is included with the attached report.

The Department of Audit Services appreciates the contribution of time and other resources from employees of the Department of Technology Solutions in the completion of this audit.

## **TABLE OF CONTENTS**

---

<b><u>BACKGROUND INFORMATION</u></b>	<b>5</b>
<b><u>EXECUTIVE SUMMARY</u></b>	<b>7</b>
<b><u>OBJECTIVES, SCOPE AND METHODOLOGY</u></b>	<b>8</b>
<b><u>AUDIT RESULTS</u></b>	<b>11</b>
<b><u>RECOMMENDATIONS</u></b>	<b>15</b>
<b><u>MANAGEMENT'S RESPONSE</u></b>	<b>16</b>

## BACKGROUND INFORMATION

---

Implementing adequate user access controls in an organization can help ensure that users have access to the right data. Access control involves three processes: authentication, authorization and audit. The focus of the audit was on the authorization and auditing processes as it relates specifically to the Department of Technology Solutions employees.

Authentication is the process of verifying the identity of the person or device attempting to access the system. The objective is to ensure only legitimate users can access the system.

The second process, authorization, restricts access of authenticated users to specific portions of the system and limits what actions they are permitted to perform. The Department of Technology Solutions implements authorization controls by using a Role Based Security Model. Role Based Access Control is a system for controlling which users have access to resources based on the role of the user. Roles are created and assigned a group of permissions. Permissions and security settings determine the programs and options available to the particular roles. The Roles are then assigned to users. A deny-all-except security policy is in use, meaning users must be initially granted specific rights through his or her roles to gain access to secured resources.

Auditing, the third process in access controls, creates a user activity trail. Administrators can analyze the audit trail and identify access anomalies that might reveal inappropriate access assignments on the part of administrators or unauthorized access attempts on the part of users.

## BACKGROUND INFORMATION

---

The Department of Technology Solutions has several standard operating procedures (SOPs) that govern user access. These SOPs are:

- *Privileged User Access Control*
- *Privileged User Access Control Local Administrator Account*
- *Physical Access Control*
- *Systems Change Control*
- *User Authorization, Identification & Authentication Control*
- *Remote Access Control*
- *Vendor Access Control*
- *SharePoint Site Collection Administrator and Site Owner Access*
- *GIS Databases Access Controls*
- *iLegislate System Access Controls*
- *Password Controls*
- *MUNIS ERP Financial System Access Control*
- *OnBase System User Groups Access Control*
- *MUNIS Database Connectivity Access Control*
- *Cellular Endpoint Web Portal Access*
- *SSRS Reports Access Control*

## EXECUTIVE SUMMARY

---

### **Purpose**

The purpose of the audit was to determine the adequacy of user access controls at the Department of Technology Solutions and verify that employees of the Technology Solutions Department have access consistent with their job responsibilities.

We conducted this performance audit in accordance with generally accepted governmental auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and 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.

### **Results in Brief**

Overall, the Department of Technology Solutions has adequate user access controls to ensure each employee's access is consistent with his or her job duties.

### **Activities that are being carried out effectively include:**

- Employee access is consistent with job descriptions;
- Management has adequate controls to monitor user access;
- The Department has written standard operating procedures governing user access;
- Adequate controls exist over access to the physical locations of the data center.

### **Areas for improvement include:**

- The standard operating procedures need revision.

## OBJECTIVES, SCOPE AND METHODOLOGY

---

### Objectives

The objectives of the audit were to:

- Determine if adequate controls exist to ensure access is granted on a need-to-know basis;
- Analyze user access and test for consistency with staff responsibilities;
- Verify the adequacy of the monitoring process.

### Scope

The scope of the audit included all current practices at the Department of Technology Solutions as they related to user access controls.

### Methodology

In order to achieve the objectives of the engagement, audit staff performed the following steps and procedures:

1. Obtained and reviewed standard operating procedures;
2. Obtained the list of authorized personnel with access to the physical location of the data center and verified that:
  - a. Employees who no longer require access are immediately removed from the list
  - b. The list is reviewed and updated on at least an annual basis
  - c. Access to the physical location is monitored;
3. Documented all systems managed by Department of Technology Solutions;

## OBJECTIVES, SCOPE AND METHODOLOGY

---

4. Randomly selected eight Department of Technology Solutions employees and verified their access as documented in the list provided by the Department of Technology Solutions;
5. Reviewed documentation for additions/changes/deletions to the privileged user groups to ensure proper approval was received;
6. Obtained the Role Based Access Control list (specifies access by employee);
7. Obtained and reviewed job descriptions for Department of Technology Solutions employees;
8. Compared employees' job descriptions to their system access as per the Role Based Access Control list and determined if access is consistent with the job descriptions;
9. Obtained a listing of personnel changes resulting from resignations, transfers or demotions in the Department of Technology Solutions during FY 2012 and verified that employee access was changed to reflect the new privileges;
10. Obtained a listing of vendors that have access to City of Durham's Information Resources (IR) and support services;
11. Verified that adequate vendor access procedures exist;
12. Obtained information on access granted to the County for City systems;

## OBJECTIVES, SCOPE AND METHODOLOGY

---

13. Documented the monitoring process;
14. Obtained and reviewed management reports used to monitor access and determined if they are adequate;
15. Determined if periodic and documented reviews are performed to evaluate the levels of access that have been granted to system users; and
16. Verified documentation for emergency and non-emergency changes to the information system and determined if the Department of Technology Solutions followed the *Systems Change Control* procedures as outlined in the standard operating procedures.

During the audit, staff also maintained awareness to the potential existence of fraud.

## AUDIT RESULTS

---

**Activities that are being carried out effectively include:**

**Overall, the Department of Technology Solutions has adequate user access controls to ensure that each employee's access is consistent with his or her job duties.**

**Employee access is consistent with job descriptions.**

Audit staff compared job descriptions to actual access for 29 Technology Solutions employees to ensure access was consistent with each job description. One exception was noted where the access was not consistent with the job description. However, according to the Department of Human Resources and Technology Solutions, the position is in the process of being reclassified. A description of the reclassified position was not available for review. The recommendation is included on the agenda item pending City Council approval at the August 6, 2012 City Council meeting. The job description for the position will be completed before the City Council meeting.

**Management has adequate controls to monitor user access.**

Each morning the Deputy Director reviews reports from Netwrix, an auditing software tool that captures changes made to the systems and servers. Reports are reviewed to identify anomalies that might reveal inappropriate access assignments on the part of administrators or unauthorized access attempts on the part of users. In addition, the Deputy Director also reviews user access privileges twice a year.

**The department has written standard operating procedures governing user access.**

## AUDIT RESULTS

---

### **Adequate controls exist over access to the physical locations of the data center.**

The Department uses a biometric scanner to keep the data center secure. The Director reviews a report from the biometric scanner weekly to monitor access to the data center.

### **Areas for improvement include:**

**Finding 1: The standard operating procedures need revision**

### **Revise the *Systems Change Control* standard operating procedure.**

At present, the Department of Technology Solutions does not follow the procedure related to performing emergency changes as defined in the standard operating procedure. Per Kerry Goode, approver of the *Systems Change Control* standard operating procedure, Requesters of emergency changes must complete an emergency change request document that must be reviewed and approved prior to emergency changes. The document should contain a brief explanation of why the change must be handled in an emergency manner, the description of the problem, proposed solution and risks<sup>1</sup>. Currently, staff notifies management of the emergency via email, text or phone. The event is documented once the problem is resolved. The emergent nature of the situation does not allow the employees to prepare documentation and get approval prior to taking corrective action as stated in the standard operating procedure. The standard operating procedure should reflect the actual procedure that is currently in practice at the department.

<sup>1</sup>Goode, K. (2012). *Systems Change Control*. Technology Solutions Department, City of Durham, North Carolina, p. 3

### **Revise the *Vendor Access Control* standard operating procedure.**

This standard operating procedure establishes the rules for vendor access to the City of Durham's Information Resources and support services. Setting limits and controls on what information the vendor can see, copy, modify, and control will eliminate or reduce the risk and liability for the City of Durham. The CIO and Deputy Director of Technology Solutions control the access to the City's network. At the time of fieldwork, seven contractors /consultants had access to the City of Durham's information resources and/or support services according to a list provided by the Department of Technology Solutions. Five of the seven contractor's access privileges according to the list never expire. Assigning a contractor access which never expires increases the risk to the City, especially if proper controls are not established to disable access once the contractor is no longer providing services to the City.

Per the Department of Technology Solutions staff, the "City provides some services, which are available to and used by the public seven days a week, 24 hours a day. These services would have a major impact on the City's service to the public should they not be available. Contract negotiations may sometimes cause the service contract to expire, while the service is still in use. For this reason the Department of Technology Solutions does not put an expiration date on these services due to the possible impact. The length of time to keep an account active is determined on an individual basis. They currently work with each customer to determine the period of access". The standard operating procedure at present does not outline how to define the period of access and any exceptions to the general rule. In addition, this standard operating procedure should provide clear guidance for access withdrawal once the contractor is no longer providing service to the City.

### **Clarify the standard operating procedure *Privileged User Access Control*.**

Currently the standard operating procedure titled *Privileged User Access Control* provides guidance to prevent inappropriate use of the privileged access by those with elevated rights to information systems and data in performing their normal duties. The CIO and Deputy Director of Technology Solutions control access to the privileged user group. The standard operating procedure defines additional requirements associated with being the domain administrator, account operator or local administrator groups on the City's domain. There are other privileged user groups, which are not specifically referenced. According to the department, the standard operating procedure is intended to apply to all roles established in the Role Based Access Control System. The standard operating procedure should clarify the definition of the privilege user group.

The procedure also states that the domain administrator, local administrator and/or account operators groups shall be reviewed by applicable technology operations staff to ensure only authorized users are part of these groups. At present, the review is performed semi-annually. The standard operating procedure does not address the review process for other role-based groups.

During fieldwork, the Department of Technology Solutions provided the Audit Services Department staff the Role Based Access Control list, which details employee access by role. The list was not complete. The Department of Technology Solutions updated the list during the field work to include the missing information identified. The department currently uses this list to monitor access. The standard operating procedure does not mention the use of this list as a monitoring tool.

## RECOMMENDATIONS

---

### Recommendation 1

Revise the standard operating procedures to include the following:

- Update the *Systems Change Control* standard operating procedure to reflect the current practice followed to address emergencies. Also, describe the documentation process for emergencies;
- Revise the *Vendor Access Control* standard operating procedure to address determination of length of vendor access to City of Durham's information resources and support services;
- Revise the *Privileged User Access Control* standard operating procedure to clarify all roles that are part of the privilege user group. In addition, define the review process for all role-based groups; and
- Include the use of a role based access control list that details employee access as part of the *Privilege User Access Control* standard operating procedure.

## MANAGEMENT'S RESPONSE



CITY OF  
DURHAM

Memo to: Germaine F. Brewington, Director of Audit Services  
From: Kerry Goode, CIO/Director  
Technology Solutions Department  
Date: August 15, 2012  
Subject: Management's Response  
**Technology Solutions Access Controls Performance  
Audit (July 2012)**

The following is management's response to the Technology Solution Controls Performance Audit (July 2012).

### **Recommendation 1**

Revise the standard operating procedures to include the following:

- Update the *Systems Change Control* standard operating procedure to reflect the current practice followed to address emergencies. Also, describe the documentation process for emergencies;
- Revise the *Vendor Access Control* standard operating procedure to address determination of length of vendor access to City of Durham's information resources and support services;
- Revise the *Privileged User Access Control* standard operating procedure to clarify all roles that are part of the privilege user group. In addition, define the review process for all role-based groups; and
- Include the use of a *Role Based Access Control* list that details employee access as part of the Privilege User Access Control standard operating procedure.

### **Management's Response:**

We concur. Management is in full agreement with the recommendation and will make the modifications to the Technology Solutions (TS) standard operating procedures (SOPs) by August 31, 2012. The affected TS staff will also be educated on the changes to the TS SOPs.