METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

OFFICE OF INTERNAL AUDIT

Professional Audit and Advisory Service

FINAL REPORT

Audit of the Acceptable Use of Information Technology Assets – Metro Action Commission

Date Issued: February 8, 2013

Office Location and Phone Number

222 3rd Avenue North, Suite 401
Nashville, Tennessee 37201
615-862-6110

The Metropolitan Nashville Office of Internal Audit is an independent audit agency reporting directly to the Metropolitan Nashville Audit Committee

EXECUTIVE SUMMARY
February 8, 2013

Results in Brief

An audit of the *Acceptable Use of Information Technology Assets Policy* for the Metro Action Commission (MAC) was chosen along with two other entities to determine progress in meeting management's goal to enhance the overall information security posture for the Metropolitan Nashville Government. This report contains the results for the Metro Action Commission.

Audit Objectives

- *Were users storing sensitive Metro Nashville information on authorized storage devices?*

  Yes. Interviewing personnel and studying the data flows of the Metro Action Commission operations demonstrated sensitive data, which includes confidential data, was stored according to the Acceptable Use Policy and best security standards.

- *Were employees knowledgeable of Acceptable Use of Information Technology Assets Policy and related Data Classification Policy provisions?*

  Generally yes. Metro Action Commission's personnel were generally knowledgeable of the Acceptable Use Policy. As a group, they did not have an awareness of the Information Classification Policy, referenced in the Acceptable Use Policy.

- *Were prohibited acts, outlined in the Acceptable Use Policy, being carried out on Metro Nashville equipment?*

  No. Employee personal use accounted for minimal time on the internet and negligible computer workstations resources. Intellectual property rights were in evidence for all installed software on department workstations.

Background and Recommendations

A new *Acceptable Use of Information Technology Assets Policy* was distributed in May 2011 and went into effect in November 2011. The purpose of the policy was to improve information security management within the Metropolitan Nashville Government.

Information Classifications

Public – No risk such as reports meant for public distribution.

Internal – Lowest risk such as staff phone numbers.

Confidential – High risk such as social security and credit card numbers.

Restricted– Highest risk where loss of life could occur, such as witness protection information.

Recommendations

Key recommendations of this report include:

- Reemphasize with the staff, the lack of expectation of privacy when using Metro Nashville technology assets.
- Review and train staff on the use of the Information Classification Policy, which is called out in the Acceptable Use of Information Technology Assets.
- Ensure staff is aware and uses only Metro-supplied removable media and cell phones, /PDAs/Blackberries.

TABLE OF CONTENTS

INTRODUCTION

Audit Initiation

The audit of the Metro Action Commission was conducted as part of the approved 2012 Audit Work Plan. The Metro Action Commission Management, located in the Clifford-Allen Building, was chosen by the Metropolitan Nashville Office of Internal Audit along with two other entities to determine progress in meeting management's goal to enhance the overall information security posture for the Metropolitan Nashville Government

Background

The Acceptable Use of Information Technology Assets Policy (hereinafter referred to as "Acceptable Use Policy") was generated from the effort established by Executive Order Number Five, Security Awareness, and Executive Order Number 38, Information Security Management Policy and Steering Committee Authorization. A team made up of representatives from all major departments collaborated to create a set of security policies and plans to improve information security management.

The purpose of this policy was to define good practices for the acceptable use of information and assets associated with information processing and information processing facilities to ensure that the Metropolitan Nashville Government achieves and maintains appropriate protection of its information technology assets.

The Metro Action Commission has 307 employees in the department. We sampled 29 persons, with ten of those having their own computer and network account. The remaining 19 shared a computer at their work site.

Organizational Structure

There are six functions reporting to the Director. Those six functions were Human Resources, Financial Operations, Administrative Services & Operations, Head Start, Early Head Start, and Community Programs. There was one main office and seven Head Start centers throughout Davidson County.

Information Systems

The following information systems were used by the Metro Action Commission staff:

- Child Plus Software – tracked family and child data for the Head Start and Community Services functions.

- THO software tracked LiHEAP (Low-income Home Energy Assistance Program), CSBG (Community Service Block Grant) programs.

There were 161 computers assigned to the Metro Action Commission staff, with 76 Multiuser and 85 individually assigned computers. There were 323 user accounts in the Active Directory database. For fiscal year 2012, information technology related budgeted expense was $135,454.

OBJECTIVES AND CONCLUSIONS

1. *Were users storing sensitive Metro Nashville information on authorized storage devices?*

   Yes. Interviewing personnel and studying the data flows of the Metro Action Commission operations demonstrated sensitive data, which includes confidential data, was stored according to the Acceptable Use Policy and best security standards. In the Head Start Centers, sensitive data was in paper form and was stored in locked file cabinets.

2. *Were employees knowledgeable of the Acceptable Use Policy and related Data Classification Policy provisions?*

   - *Were users aware of password requirements?*
   - *Were user's email and internet access primarily for Metro Nashville business purposes?*
   - *Were user's mobile phones authorized by Metro Nashville and connected to an approved mobile device server?*
   - *Were user's expectations of privacy, when using Metro Nashville devices, valid?*
   - *Were users accessing the Metro Nashville network from an external site utilizing an approved virtual private network connection?*

   Generally yes. Metro Action Commission's personnel were generally knowledgeable of the Acceptable Use Policy. As a group, they did not have an awareness of the Information Classification Policy, referenced in the Acceptable Use Policy, part 2.1 (See Observation A).

   Furthermore the following security practices were observed:

   - Passwords and logical locks were applied according to the Acceptable Use Policy.
   - There was no evidence that email was being used for non-business purposes based on interviews and direct observation of email content.
   - Users were aware of the internet access requirements.
   - Metro Nashville approved cell phones, personal digital assistants, smart phones or removable media devices were being used, in all but one instance (See Observation A).
   - Users expected their data to be private versus the policy which states it was not for nine of 29 (31 percent) of sample employees (See Observation A).
   - Users with remote access privileges agreed with the active directory security group members list.

The Metro Action Commission had been exposed to the Acceptable Use of Information Technology Assets policy and employees were generally aware of and had signed-off on the policy.

While a group of Metro Action Commission personnel were aware of the Information Classification Policy, only one person could describe the contents of the policy.

3. *Were prohibited acts, outlined in the Acceptable Use Policy, being carried out on Metro Nashville equipment?*

    - *Excessive personal use*
    - *Viewing or storing inappropriate material*
    - *Illegal duplication of software*
    - *Unauthorized system access*
    - *Unauthorized distribution of information on the internet*

    No. Employee personal use accounted for minimal time on the internet and negligible computer workstations resources. Intellectual property rights were in evidence for all installed software on Metro workstations.

OBSERVATIONS AND RECOMMENDATIONS

A - Acceptable Use of Information Technology Assets Policy

Information security practices could be improved to minimize the risk of unauthorized access or processing of Metro Nashville information assets. The following areas of concern were observed:

- Staff indicated they had an expectation of privacy when sending and receiving data or email. This was the case for nine of 29 (31 percent) of the Metro Action Commission users. The remaining personnel did not expect privacy in those instances, because, data could be sent anywhere, seen by anyone or requested through e-discovery by the Department of Law or open records requests.
- Metro Action Commission's personnel were generally knowledgeable of the Acceptable Use Policy. As a group, they did not have an awareness of the Information Classification Policy, referenced in the Acceptable Use Policy, part 2.1 (Sensitive Information User Responsibility)
- The Acceptable Use Policy, parts 8.0 (Removable Media) and 10.0 (Approved Cell Phones, PDAs or Blackberries) have not been sufficiently communicated to all personnel. In the interviews and surveys, users were not aware of these parts of the policy. There was one employee using a removable device brought from home which is not recommended in the Removable Media part of the Acceptable Use Policy.

Criteria:

- *Acceptable Use of Information Technology Assets Policy*, 7.1.3, effective November 1, 2011
- *Information Classification Policy*
- ISO 27002, Part 11.1, Access control rules should take account of policies for information dissemination and authorization.

Risk:
Unauthorized access or processing of Metro Nashville information may occur resulting in financial loss or compromise of public trust.

Recommendation:
Management of the Metro Action Commission should:

1. Reemphasize with staff of the lack of expectation of privacy, when using Metro Nashville technology assets.
2. Train staff on the use of the Information Classification Policy.
3. Ensure staff is aware and uses only Metro-supplied removable media and cell phones/PDAs/Blackberries.

GENERAL AUDIT INFORMATION

Statement of Compliance with GAGAS

This audit was conducted from August 2012 to October 2012, 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 observations and conclusions based on our audit objectives.

We believe that the evidence obtained provides a reasonable basis for our observations and conclusions based on our audit objectives.

Scope and Methodology

The audit period focused primarily on the period November 1, 2011, through June 30, 2012. The methodology employed throughout this audit was one of objectively reviewing various forms of documentation, conducting interviews and surveys, observations, procedures, and other relevant data.

Criteria

In conducting this audit, the existing processes were evaluated for compliance with:

- *Acceptable Use of Information Technology Assets Policy*, 7.1.3, effective November 1, 2011
- *Information Classification Policy*, 7.2,1, effective November 1, 2011
- *International Standards Organization 27001/27002*, Part 7

Audit Project Staff

Joseph McGinley, CISSP, CISA - In Charge Auditor
Mark Swann, CPA (Texas), CIA, CISA – Quality Assurance

APPENDIX A. MANAGEMENT RESPONSE

Management's Responses Starts on Next Page

KARL F. DEAN, MAYOR

METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY

Cynthia L. Croom
Executive Director

METROPOLITAN ACTION COMMISSION
800 2nd Avenue North
Nashville, TN 37201
Mailing Address: Post Office Box 196300
Nashville, Tennessee 37219-6300
Phone (615) 862-8860
Fax (615) 862-8881
www.nashville.gov/mac

February 8, 2013

Office of Internal Audit
Mr. Mark Swann, Metropolitan Auditor
1417 Murfreesboro Rd.
Nashville, TN 37217

Dear Mr. Swann:

On behalf of the Metropolitan Action Commission, I have reviewed and accepted the audit of Acceptable Use of Metropolitan Nashville Information Technology Assets for the Metropolitan Action Commission. We appreciate your department's time and professionalism in the audit process.

The management and staff of the Metropolitan Action Commission will greatly benefit by performing the recommended training and corrections cited in the report.

Sincerely,

Cynthia Croom

The community action agency for Nashville and Davidson County

Community Action changes people's lives, embodies the spirit of hope, improves communities, and makes America a better place to live.
We care about the entire community and are dedicated to helping people help themselves and each other.

Audit of the Acceptable Use of Information Technology Assets Policy
Metro Action Commission Response to Audit Recommendations

Audit Recommendation	Response to Recommendation/Action Plan	Assigned Responsibility	Estimated Completion
A.1.Reemphasize with staff of the lack of expectation of privacy, when using Metro Nashville technology assets.	**Accept.**	Executive Director	
A.2 Train staff on the use of the Information Classification Policy.	**Accept.**	Executive Director	
A.3 Ensure staff is aware and uses only Metro-supplied removable media and cell phones/PDAs/Blackberries.	**Accept.**	Executive Director	