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 – Nashville Expo Center

Date Issued: September 28, 2012

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
September 28, 2012

Results in Brief

An audit of the *Acceptable Use of Information Technology Assets Policy* for the Tennessee State Fair-Nashville Expo Center 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 Tennessee State Fair-Nashville Expo Center.

Audit Objectives

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

  Yes. According to the *Acceptable Use Policy*, Nashville Expo Center employees have taken measures to protect sensitive information from loss or exposure.

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

  Generally yes. The Nashville Expo Center employees were generally aware of the *Acceptable Use Policy*. Most users were following the policy. There were two areas in which 50 percent of the department did not follow policy provisions; password storage and expectation of privacy.

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

  No. According to the policy, employee personal use accounted for minimal time on the internet and there was no evidence of inappropriate activity.

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

- Ensure user accounts and passwords are not displayed at work sites.
- Contact the Information Technology Services Help Desk when access to a staff members files are necessary. Only the assigned user should have access to their account and password.
- Provide additional training on secure encryption communication techniques.
- Enable the automatic screen lock after fifteen minutes of inactivity for all computer workstations.

TABLE OF CONTENTS

INTRODUCTION

Audit Initiation

The audit of the Tennessee State Fair - Nashville Expo Center was conducted as part of the approved 2012 Audit Work Plan. The Tennessee State Fair-Nashville Expo Center (hereinafter referred to as the "Nashville Expo Center") located at the Tennessee State Fairgrounds, 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.

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 Nashville Expo Center has 17 full time employees, of which 11 have computer access. Each of the 11 employees has their own computer and network computer account and is aware of and has signed the *Acceptable Use Policy*.

Organizational Structure

There is a five-member Board of Fair Commissioners which is responsible for governance and oversight for the Director of the Nashville Expo Center.

Information Systems

The following information systems are used by the Nashville Expo Center staff:

- UV Term - Flea Market: Customer data base
- Link2Gov - Flea Market: Used for credit card authorization
- Treasury Banking Software - Flea Market: Cash deposits
- Microsoft Office - Corporate Sales: Purchasing, contracting, letter writing
- Enterprise Business Systems Accounting and Human Resources – Accounting and Fair Director: Cost accounting and employee management
- Maintenance / Inventory System - Building Maintenance: Maintenance requests and inventory system

For fiscal year 2012, information technology related budgeted expense was $64,500.

OBJECTIVES AND CONCLUSIONS

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

Yes. According to the *Acceptable Use Policy*, Nashville Expo Center employees have taken measures to protect sensitive information from loss or exposure. Interviews and direct observation verified that this information, which included confidential employee, medical, financial and purchasing documents, was protected. Approximately 90 percent of the information was stored on paper and was locked in department file cabinets, with access assigned to need to know personnel only.

The Flea Market Business Office conducted credit card sales over the phone and wrote down the credit card number from the caller before entering the number into the computer. Nashville Expo Center employees stated credit card information was shredded immediately after the transaction was complete.

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. The Nashville Expo Center employees were generally aware of the *Acceptable Use Policy*. Most users were following the policy. There were two areas in which 50 percent of the department did not follow policy provisions; password storage and expectation of privacy. There was one occurrence of multiple parts of the policy not being followed for daily computer processing needs (see Observation A).

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. According to the policy, Nashville Expo Center employee personal use accounted for minimal time on the internet and there was no evidence of inappropriate activity.

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:

- One employee had posted their password on the computer screen to be used by co-workers to access information stored on their computer.
- Employee network passwords were stored in a paper file for the entire department in the event an employee was not available. Computer account passwords should only be used by the individual assigned to the account.
- Employees indicated they understood communication using email or file transfers would always remain private between the employee and the recipient.
- One computer did not have the screen lock after fifteen minutes of inactivity feature enabled. This was the practice to facilitate the receipt of fax communications.

Criteria:
Acceptable Use of Information Technology Assets Policy, 7.1.3, effective November 1, 2011

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

Recommendation:
Management of the Nashville Expo Center should:

1. Ensure user accounts and passwords are not displayed at work sites.
2. Contact the Information Technology Services Help Desk when access to staff members' files are necessary. Only the assigned user should have access to their account and password.
3. Provide additional training on secure encryption communication techniques.
4. Enable the automatic screen lock after fifteen minutes of inactivity for all computer workstations.

GENERAL AUDIT INFORMATION

Statement of Compliance with GAGAS

This audit was conducted from June 2012 to July 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, performing substantive tests and tests of internal controls on the entity's information assets, written policies and procedures, contracts 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 Polic*y, 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

Nashville Expo Center
The Place To Show & Sell

September 14, 2012

Mr. Mark Swann
Metropolitan Auditor
Office of Internal Audit
222 3rd Avenue North, Suite 401
Nashville, TN 37201

Re: Compliance Audit of the Tennessee State Fairgrounds/Nashville Expo Center

Dear Mr. Swann:

On behalf of the Tennessee State Fairgrounds/Nashville Expo Center, I acknowledge receipt of the Internal Audit Working Paper for our requested Compliance Audit. We assent to all findings and recommendations and, as you will see in the accompanying report, have begun a series of responses to address each recommendation.

We appreciate and look forward to your continued support as we move toward full compliance in a timely and thorough manner. It has been a pleasure to work with Mr. McGinley and your staff. Please let us know if you need any additional information.

Sincerely,

Buck Dozier

Buck Dozier
Executive Director Tennessee State Fairgrounds/Nashville Expo Center

P.O. Box 40208 Nashville, TN 37204 Office (615) 862-8980 Fax (615) 862-8992
www.nashvilleexpocenter.org

Audit of the Nashville Expo Center Acceptable Use of Information Technology Assets Policy
Management Response to Audit Recommendations

Audit Recommendation	Response to Recommendation/Action Plan	Assigned Responsibility	Estimated Completion
A. Management of the Nashville Expo Center should: 1. Ensure user accounts and passwords are not displayed at work sites.	**Accept –** Password displayed in open area has been removed and employee has been instructed on the importance of keeping passwords secured and private.	Laura Faust	9/14/12 Completed
2. Contact the Information Technology Services Help Desk when access to a staff members files are necessary. Only the assigned user should have access to their account and password.	**Accept –** All passwords in the folder have been destroyed and it has been communicated to employees that if access to another person's computer is needed it must be done through Metro IT.	Laura Faust	8/31/12 Corrected during the audit
3. Provide additional training on secure encryption communication techniques.	**Accept –** All employees will be instructed on the encryption process by the end of December, 2012. An email will be sent out explaining the process and any employee interested will be encouraged to attend training at the next available opportunity.	Kristi Harris	12/31/12
4. Enable the automatic screen lock after fifteen minutes of inactivity for all computer workstations.	**Accept –** The PC that had this issue was extremely old and was on a list to be replaced. The PC has since been replaced with another surplus PC from Metro IT	Laura Faust / Steve Burton	8/31/12 Completed