mesa·az
CITY AUDITOR
mesaaz.gov

20 E Main St Suite 820
PO Box 1466
Mesa, Arizona 85211-1466

Date: January 13, 2014

To: Audit, Finance and Enterprise Committee

From: Jennifer Ruttman, City Auditor

Subject: Final Report – Annual Credit Card Security Review

cc: Michael Kennington, CFO
Alex Deshuk, Manager of Technology & Innovation
Natalie Lewis, Assistant to the City Manager
Irma Ashworth, Finance Director
Heather Wolf, Library Director
Cindy Ornstein, Arts & Culture Department Director

Pursuant to the Council-approved Audit Plan, the City Auditor's office has completed our annual credit card security review. The attached report includes recommendations to 3 departments and corresponding responses from management. The report will be presented at the next scheduled meeting of the Audit, Finance and Enterprise Committee. Please feel free to contact me with any questions or concerns.

mesa·az
CITY AUDITOR
mesaaz.gov

20 E Main St Suite 820
PO Box 1466
Mesa, Arizona 85211-1466

FINAL REPORT **CITY AUDITOR**

Report Date:	**January 13, 2014**
Department:	**Citywide**
Subject:	**Annual Credit Card Security Review**
Lead Auditor:	**Dawn von Epp**

OBJECTIVES

Our annual credit card security review is an assessment of the City's operational efforts to protect customers' credit card information, as required by the Payment Card Industry's Data Security Standard (PCI DSS). Specifically, our objectives were to determine whether:

- City departments maintain and enforce policies and procedures that meet PCI DSS requirements.
- Individuals who handle credit card information are adequately screened and trained.
- Management has effectively implemented all corrective action plans developed in response to prior PCI DSS reviews.

SCOPE & METHODOLOGY

This review focused on the operational (non-IT) requirements of PCI DSS, which apply to credit card handling activities at the City's 31 credit card acceptance sites. To accomplish our objectives, we interviewed staff members; observed operations and processes; and reviewed policies, procedures, document inventories, and training records.

BACKGROUND

As a merchant that accepts credit cards, the City is required to comply with PCI DSS. Failure to do so could place our customers at risk for identity theft and could result in credit card companies levying fines or prohibiting the City from accepting credit card payments. To help ensure compliance citywide, the Accounting Services Division is responsible for maintaining Management Policy 212 – Credit Card Handling (MP 212) and training individuals on PCI DSS requirements and credit card handling procedures. They also manage the City's merchant accounts. The Information Technology Department (ITD) is responsible for ensuring the City's compliance with the IT-related requirements of the PCI DSS.

CONCLUSION

We have conducted five credit card security reviews since 2008 and significant progress has been made in the overall effort to fully comply with PCI DSS. However, there are a few concerns that have surfaced during all five reviews. These concerns generally relate to timely and effective destruction of credit card data, secure storage of such data prior to destruction, and management of passwords on credit card terminals. Although individual instances have been addressed when identified, it is our opinion that the recurring nature of these issues is indicative that there are insufficient controls in place to ensure ongoing compliance. Therefore, in addition to making recommendations to bring these departments into compliance, we have asked the City Manager's office to clearly communicate the need for, and expectation of, ongoing compliance in the future.

RECOMMENDATIONS

The following are our specific recommendations, listed by department, along with responses from the respective department managers. We will follow-up on their status during next year's review.

Arts & Culture, Arizona Museum for Youth (AMY)

Recommendations: AMY should ensure that current fiscal year credit card receipts are secured at all times and that credit card records that exceed the retention schedule are destroyed. In addition, the Friends of AMY credit card terminal should be configured to require a password to process refunds. All credit card terminal passwords should be actively managed to ensure that passwords are known only by employees who need them to perform their job duties, and that passwords are changed periodically, including when there is staff turnover or when the passwords are thought to have been compromised.

Management Response: AMY has secured current year credit card receipts in a locked filing cabinet, and has destroyed all other credit card records. The Friends of AMY credit card terminal is now password protected when a refund is required.

Financial Services, Accounting Services Division

Recommendations: Accounting Services Division should destroy the numerous credit card documents stored by the City's off-site provider that are now well beyond the retention date. At the time of this review, there were at least 196 cartons known to contain credit card data that were past due for destruction (i.e. more than 7 years old). This has been a finding in all 5 of our PCI DSS reviews; therefore, management should also develop an improved internal control mechanism to ensure compliance with credit card document retention policies in the future.

Management Response: The cartons containing credit card documents have been destroyed. We are currently writing procedures to ensure ongoing compliance with document retention standards.

Library Services, Mesa Express Library

Recommendations: The Mesa Express Library (MEL) should ensure ongoing compliance with departmental credit card handling procedures, which require that:

1. Credit card terminal passwords are changed annually or when there is turnover of staff.
2. Transaction receipts and all other cardholder data, including balancing and audit reports, are secured at all times.

Management Response: The password for MEL's credit card terminal has been reset and will be reset again at least annually. Staff has been trained on all policies and procedures to ensure future compliance. Additionally, Management Policy 210 and 212 as well as Library procedures for cash and credit card handing will be reviewed with all library supervisors annually. Receipts are now stored in a secure location.