




PO Box 1466
Mesa, Arizona 85211-1466

mesaaz.gov/auditor

Date: January 10, 2011

To: Audit & Finance Committee

From: Jennifer Ruttman, City Auditor 

Subject: Annual Credit Card Security Review

cc: Alex Deshuk, Manager of Technology & Innovation
Doug Yeskey, Controller
Patricia Sorensen, Acting Deputy City Manager
Ed Quedens, Business Services Director
Tim Meyer, Revenue Collections Administrator
John Albin, Materials & Supply Administrator
Kari Kent, Deputy City Manager
Marc Heirshberg, PRCF Director
Natalie Lewis, Assistant to the City Manager
Corrine Nystrom, Falcon Field Airport Director
Rick Welker, Financial Coordinator

Pursuant to the Council-approved audit plan, the City Auditor's office has completed our annual credit card security review. The final report is attached.

Please feel free to contact me at x3767 or Jason Taylor at x3635 if you have any questions or comments about this report.



PO Box 1466
Mesa, Arizona 85211-1466

mesaaz.gov/auditor

SUMMARY REPORT

CITY AUDITOR

Report Date: November 15, 2010
Department: Citywide
Subject: Annual Credit Card Security Review

OBJECTIVE

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

SCOPE & METHODOLOGY

This review focused on the credit card handling operations that take place outside of the City's IT infrastructure. To accomplish our objectives, we interviewed City staff members, observed various departments' operations and processes, reviewed document inventories from the City's offsite storage vendor, and reviewed attendance records for the City's Credit Card Handling training class.

BACKGROUND

As a merchant that accepts credit cards, Mesa is required to comply with the PCI DSS. Failure to comply with this standard could result in the credit card brands levying fines or prohibiting the City from accepting credit card payments. Since most of the PCI DSS requirements center on information technology, ITD launched a project in 2006 to bring the City into compliance. ITD adopted the PCI Security Council's prioritized approach for ensuring compliance. The department has implemented the most critical requirements for protecting the City's electronic credit card data, and is now focusing on the lower priority goals. Another key department involved with ensuring PCI DSS compliance is the Accounting Services Division. Accounting Services manages the City's merchant accounts, continually develops Management Policy 212 (*Credit Card Handling*), and trains employees on credit card handling procedures and PCI DSS requirements.

CONCLUSION & RECOMMENDATIONS

Since our first annual review in 2008, most departments have implemented our recommendations to bring their operations into compliance, and we commend their efforts and cooperation. However, at the time of this review, we found that five departments had not implemented the recommendations, despite either having agreed to do so or having asserted that they had already done so. While we understand that these departments are faced with heavy workloads, and some are actively involved in the CityEdge project, many of these recommendations would have taken only a few hours to implement after the prior review(s).

Due to the sensitive nature and security concerns associated with credit card operations, this report does not include the specific findings and recommendations that we found to be unresolved or unimplemented during our review. However, we reported these deficiencies in detail to the City Manager and to the departments in which they were found. Since that time, all of these departments have responded appropriately and have either made the requested changes or are in the process of doing so. As stated above, most of the changes were not time-consuming; they simply needed to become a priority. We will follow up again during the 2011 annual review.