mesa·az
OFFICE OF THE CITY CLERK

AUDIT, FINANCE & ENTERPRISE COMMITTEE

February 4, 2014

The Audit, Finance & Enterprise Committee of the City of Mesa met in the lower level meeting room of the Council Chambers, 57 East 1st Street, on February 4, 2014, at 10:00 a.m.

COMMITTEE PRESENT	COMMITTEE ABSENT	STAFF PRESENT
Alex Finter, Chairman	Christopher Brady, Ex Officio	Alfred Smith
Scott Somers		Natalie Lewis
Dave Richins		

Chairman Finter excused Committeemember Richins from the beginning of the meeting; he arrived at 10:06 a.m.

1. Items from citizens present.

There were no items from citizens present.

2-a. Hear a presentation, discuss and provide a recommendation on the following audit:

1. Annual Credit Card Security Review

City Auditor Jennifer Ruttman reported that this audit **(See Attachment 1)** relates to the annual Payment Card Industry's Data Security Standard (PCI DSS). She explained that the review focuses 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. She stated that it was important to determine whether the current processes and procedures in place at those locations are, in fact, protecting City customers' credit card information.

Ms. Ruttman commented that this audit has been performed on an annual basis for the last five years and noted that although significant progress has been made in the overall effort to fully comply with PCI DSS, the audit has revealed "some repeat findings" in a few City departments. She remarked that her office made a concerted effort this year to work with those departments to ensure that the issues are corrected so that future reviews "will be clean." She added that the City Manager's Office was asked to communicate to those departments the need for, and expectation of, ongoing compliance in the future.

Ms. Ruttman pointed out that when City departments experience turnover in staff, it is often difficult for the new employees to understand the procedures with regard to the secure storage of credit card data, as well as the securing of the credit card terminals with passwords.

Chairman Finter cited Target's recent security breach of its customers' credit card information as a prime example of why the City's annual PCI DSS audit is so crucial.

Ms. Ruttman confirmed that the security breach at Target demonstrated that the point-of-sale terminals are a point of vulnerability and prompted City staff to ensure that Mesa's credit card acceptance sites are secure.

In response to a question from Chairman Finter, Ms. Ruttman reiterated that her office has been working with the departments to develop an ongoing process to ensure future compliance.

Responding to a question from Committeemember Somers, Ms. Ruttman clarified that the City IT Department has implemented a strategic plan to maintain PCI compliance, which Assistant Chief Information Officer Pat O'Keefe oversees.

Committeemember Somers commented that the Council was recently provided a report that outlines the City's challenges with respect to IT, and noted that both information technology and communication technology are increasing at a rapid pace. He indicated that while all of the City departments "seem to be implementing their IT differently," there does not appear to be "an over-arching strategy." He suggested that the non-compliance with respect to this specific audit is "a symptom of that." He added that cyber security and bank account/credit card matters are not separate, but rather all part of the same issue.

Committeemember Somers further remarked that it would benefit staff and the Council to engage in "a global conversation" on information and communication technology, cyber security, and the security of customers' credit card information in order to move forward with the goal of securing and implementing technology "in one step." He added that this would assist the Council in being able to follow each department's efforts in this regard.

Assistant to the City Manager Natalie Lewis responded that she would share Committeemember Somers' suggestions with Manager of Technology & Innovation Alex Deshuk and ask him if he could work with the City's IT staff in an effort to compile additional information concerning this issue. She stated that staff could bring back the data to the Council on an individual basis or perhaps at a future Study Session.

Ms. Ruttman clarified that her department does not have an IT audit function and pointed out that her staff has limited their review to operational procedures. She stated that her staff communicates with the IT Department to the extent that such procedures overlap with IT's efforts, for example, in the securing of the credit card terminals, and ensuring that everyone "is on the same page." She added that the IT Department would be the more appropriate source to address technology-based solutions.

Chairman Finter concurred with Committeemember Somers' comments regarding the development of an overall global strategy and added that "there are a lot of pieces of the puzzle floating around."

Responding to comments from Chairman Finter, Ms. Ruttman advised that the departments with the repeat problems have higher turnover than other departments. She stated that it was really a management oversight issue to ensure that the managers maintain continuity over the function so that their employees comply with the policies and procedures in this regard.

In response to a question from Committeemember Richins, Ms. Ruttman clarified that the Accounting Division conducts mandatory training for new employees who will handle credit card transactions as part of their job functions.

Ms. Ruttman further indicated that staff will once again conduct an audit of this matter next year.

Chairman Finter thanked Ms. Ruttman for the presentation.

2-b. Hear a presentation, discuss and provide a recommendation on the proposed fees and charges for the Parks, Recreation and Commercial Facilities Department.

Parks, Recreation and Commercial Facilities (PRCF) Department Director Marc Heirshberg displayed a PowerPoint presentation **(See Attachment 2)** and reported that the purpose of the presentation was to review the proposed changes to fees and charges for various services provided by the PRCF Department.

Mr. Heirshberg briefly discussed the fees and charges review process (See Page 2 of Attachment 2) and noted that the Parks and Recreation Advisory Board has approved the recommended fees and charges.

Mr. Heirshberg explained that with respect to the Commercial Operations, there are no changes in the fee ranges. He clarified that what staff presents to the Committee is a series of fee ranges and noted that staff works within those ranges and sets the fees accordingly dependent upon the market.

Mr. Heirshberg advised that with respect to Recreation Operations, staff anticipates a $350 fiscal impact for FY 13/14 and for FY 14/15, a $2,000 impact. He said that certain verbiage changes and minor adjustments to ranges would be made to the resolution in order to remain competitive in the market. He further indicated that the Committeemembers were furnished detailed information relative to the proposed fees and charges, but noted that he would offer a short synopsis of those proposals.

Mr. Heirshberg remarked that with regard to the Aquatics Program, staff recommends a change to the Public Swim Punch Ticket. He stated that all of the pools will charge the same fee and pointed out that the punch ticket can be used for admission at any of the pools. He also discussed various verbiage changes that would be implemented related to the Flowrider. (See Page 4 of Attachment 2) He added that relative to park usage, staff proposes to add charges for the rental of the amphitheater at Eastmark and Dobson Ranch Parks.

Mr. Heirshberg briefly discussed the proposed fees and charges at Red Mountain Center. (See Page 5 of Attachment 2) He cited, for instance, that the issuance of passes is being restructured to eliminate those that are no longer requested and to lower the age range on other passes from age 5 to age 4. He also noted that fees will be added for enhanced fitness services and wellness seminars in order to provide additional opportunities for community engagement. He

added that concerning the climbing wall, staff recommends changing "Orientation" to "Belay Certification" and correcting the hourly fee rental, as well as rental per hour for commercial use.

Mr. Heirshberg further spoke relative to Adult Sports and Youth Sports and reported that staff recommends changing the verbiage and removing the listing of specific sports (except for Adult Softball) and setting fees and charges that will cover both current and future sports. He noted that originally, the fee schedule identified each sport individually, which restricted staff from a programming standpoint. He said that the proposal would allow for the creation of new sports and leagues as popularity increases.

Responding to a question from Chairman Finter, Mr. Heirshberg clarified that Mesa's Adult Softball program, which serves approximately 1,700 teams annually, continues to be the largest in Arizona. He explained that with the closure of Riverview Park, the number of teams has declined somewhat, but said that as part of the Parks Bond package, additional softball fields will be developed at the West Mesa Sports Complex, Kleinman Park and Powell Junior High. He added that unlike other municipalities, Mesa's Adult Softball Program is offered year-around.

Mr. Heirshberg continued with the presentation and reported that with respect to the Recreation Programs, staff recommends that the Teen Leadership Program be added to the fee schedule. He said that the fee will include program participation, field trips and other items. He also remarked that Birthday Party Packages are being modified to include additional child fees for residents and non-residents in order to allow greater flexibility.

Discussion ensued relative to the fees at the new Riverview Park, which are included in the existing fee schedule; that eventually, people will only be able to reserve two ramadas at the site; that at the present time, the ramadas are available on a first-come, first-served basis; that an open-space fee currently exists, which allows people to bring their own 10 by 10 canopy or inflatable bounce house for a birthday party; that for large events, such as a food truck festival or 5K race, the fees are listed as negotiable, since it would depend on the type of event and the services that the organizers would be providing to the community; and that the City and Mesa Public Schools (MPS) have entered into an Intergovernmental Agreement (IGA), which sets out the fees that are charged by the respective entities.

It was moved by Committeemember Richins, seconded by Committeemember Somers that the Parks, Recreation and Commercial Facilities Department's Schedule of Fees and Charges be forwarded on to the full Council for discussion and consideration.

Carried unanimously.

Chairman Finter thanked Mr. Heirshberg for the presentation.

3. Adjournment.

Without objection, the Audit, Finance & Enterprise Committee meeting adjourned at 10:25 a.m.

I hereby certify that the foregoing minutes are a true and correct copy of the minutes of the Audit, Finance & Enterprise Committee meeting of the City of Mesa, Arizona, held on the 4th day of February, 2014. I further certify that the meeting was duly called and held and that a quorum was present.

_____

DEE ANN MICKELSEN, CITY CLERK

pag
(attachments – 2)

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.

Fees & Charges Review FY 13/14 and FY 14/15

Parks, Recreation & Commercial Facilities Department (PRCF)

mesa·az

Review Process

- PRCF Department
- Parks and Recreation Advisory Board Fees and Charges Subcommittee
- Full Parks and Recreation Advisory Board
- City Council Audit, Finance and Enterprise Committee
- City Council

mesa·az

Recreation Operations

- Fiscal Impact
  - FY 12/13 - $350
  - FY 13/14 - $2,000

- Verbiage changes and minor adjustments to ranges to offer services that customers have come to expect, while remaining competitive with comparable facilities

Recreation Operations

- ***Aquatics Programs***
  - *Change Public Swim Punch Ticket* - All of the pools will be the same fee and the punch ticket can be used for admission to any of the pools.
  - *Change verbiage at FlowRider – Corrects verbiage and adds additional options for use.*
    - Hourly Admission - 17 and under and Hourly Admission - 18 and over.
    - Replace FlowRider Season Pass with 10 Punch Ticket and 30 Punch Ticket.
- ***Park Use***
  - Add charges for rental of Amphitheater at Eastmark and Dobson Ranch.

Recreation Operations

- ***Red Mountain Center***
  - *Pass restructure - T*o eliminate those that are no longer requested, expand ranges, and lower age range on some passes from age 5 to age 4.
    - Family Pass and Single Parent Pass be restructured to One (1) Adult and Two (2) Adult Family Memberships, while also adding a new fee for additional children beyond the five included with the Family Membership.
  - *Fitness and Wellness.* Add fees for Enhanced Fitness Services and Wellness Seminars in order to provide additional opportunities for community engagement.
  - *Climbing Wall.* Change Orientation to Belay Certification, correct fee for hourly rentals and add Rental per Hour-Commercial.

Recreation Operations

- ***Adult Sports and Youth Sports***
  - To change the verbiage and remove the listing of specific sports, except for Adult Softball, and set fees and charges that will cover sports; current and future.
    - This will allow for the creation of new sports and leagues as popularity and demand increase, as opposed of limiting to specific named sports.
- ***Recreation Programs***
  - Add Teen Leadership Program to schedule – Fee will include program participation, field trips, and other items for participation.
  - Birthday Party Packages - Add additional child fees for resident and non-resident to allow flexibility.

mesa·az

Questions?