mesa·az
CITY AUDITOR
mesaaz.gov

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

AUDIT REPORT

Date:	**June 10, 2020**
Department:	**Citywide**
Subject:	**Annual Credit Card Security Review**
Lead Auditor:	**Dawn von Epp**

OBJECTIVE

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:

- The City maintains and enforces policies and procedures that meet PCI DSS requirements.
- Individuals who handle credit card information are adequately screened and trained.
- When service providers are used to handle credit card information, due diligence is performed prior to engaging them, written agreements include required language, and they are monitored annually for PCI DSS compliance.
- Management has implemented corrective action plans in response to prior PCI DSS reviews.

SCOPE & METHODOLOGY

This review was focused on assessing compliance with the operational (non-IT) requirements of PCI DSS, which apply to credit card handling activities at the City's 43 credit card acceptance sites. Specific criteria and guidance for assessing compliance were provided by the PCI Security Standards Council's *Payment Card Industry (PCI) Data Security Standard Requirements and Security Assessment Procedures v3.2.1*, May 2018. To accomplish our objectives, we interviewed staff members; observed operations and processes; and reviewed policies, procedures, document inventories, contract documents, and training records.

BACKGROUND & DISCUSSION

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 providing training for individuals on PCI DSS requirements and credit card handling procedures. They also manage the City's merchant accounts. The Department of Innovation and Technology (DoIT) is responsible for ensuring the City's compliance with the IT-related requirements of PCI DSS, and for the annual submission of a Self-Assessment Questionnaire to our acquiring bank.

CONCLUSION

Prior Year Issues: Our 2019 report included several recommendations, all of which have been implemented, as briefly summarized in the following table:

Recommendation	Departments	Implemented
Remind departments new credit card handlers to complete training within 3 months, and department staff to ensure this occurs.	Financial Services Library Services	✓
Ensure cardholder data is destroyed per retention schedule.	Municipal Court	✓
Implement a secure process for receiving customer credit card numbers.	PRCF Convention Center	✓*
Utilize City contracted vendors or establish a contract in which vendor accepts responsibility for cardholder data.	PRCF (after activity transferred to them from PIO)	✓

* The Convention Center had a two-part plan to address our recommendation but was unable to fully implement the second part due to restrictions caused by the Covid-19 virus. The associated risk has been addressed but we will follow up when the Convention Center is operating again.

New/Continuing Issues: Overall, management has attempted to implement better processes to ensure continued compliance, but awareness and compliance with PCI DSS requirements has not been consistent. Some of the current issues have been identified in previous audits, although not necessarily in the same departments and/or in consecutive years. The current issues are summarized below; and additional details are presented in the attached Issue and Action Plans (IAPs). Next year's review will include follow-up testing to verify that the departments have successfully resolved the issues.

SUMMARY OF OBSERVATIONS & RECOMMENDATIONS

1. **Observation:** Staff is not accurately recording or inspecting point of sale devices as required by PCI DSS.

   Recommendation: Staff should maintain an up-to-date list of devices and conduct periodic inspections.

2. **Observation:** Credit card training is not consistently being completed by credit card handlers within the required time frames.

   Recommendation: The Arts & Culture and Parks, Recreation, and Community Facilities (PRCF) departments should implement controls to ensure that they comply with the training requirement.

Issue and Action Plan #1

Issue #1: Point of sale devices not consistently inspected and accurately recorded.

Observation: Parks, Recreation, and Community Facilities (PRCF) did not perform required inspections of point of sale (POS) devices, and the list of devices has not been corrected.

Criteria: "PCI DSS v3.2.1 Requirements and Security Assessment Procedures" includes following requirements (summarized):

- Requirement 9.9.1*: Maintain an up-to-date list of devices. The list should include make, model, location, and serial number (or other unique identifier).*
- Requirement 9.9.2: *Periodically inspect device surfaces to detect tampering or substitution.*

Minimum Required Credit Card Handling Procedures, "Monitoring Section, Item 6.e: *"Perform Quarterly inspections of all card swipe/dip devices for signs of tampering or substitution."*

Comments: If POS devices are not accurately recorded and inspected, tampering or substitution could go unnoticed, which would increase the potential impact of a breach.

Recommendation(s) and Management's Action Plan(s):

Recommendation #1-1: Staff should maintain an up-to-date list of POS devices, and use it when performing inspections.

Action Plan #1-1: The Point of Sale Device Inspections data is housed on Sharepoint and will be updated at least quarterly or when there are new, replaced or retired devices.

Individual or Position Responsible: Linda Smith

Estimated Completion Date: July 31, 2020

Recommendation #1-2: Staff should conduct and document inspections of all point of sale devices to meet both PCI DSS and City requirements.

Action Plan #1-2:

1. Each POS device has been assigned a location contact person. PRCF IT (Linda) will contact the assigned person via phone on a quarterly basis (based on the Fiscal Year) to verify device location and number and guide them through the inspection process.

a. As part of each inspection, the contact person will take a picture of the device and submit it to Linda via email.
    i. The photos will be stored on the share drive for audit purposes.

2. All POS devices will be inspected quarterly, with the exception of the pool locations that are closed for the off-season (i.e., all pools except Skyline and Kino – due to year round lap swim) and the Merry Main Street devices. The exempt locations will be audited during the quarters the devices are in use (Pools - Q1 & Q4; Merry Main St – Q2)

Individual or Position Responsible: Linda Smith

Estimated Completion Date: July 31, 2020

Issue and Action Plan #2

Issue #2: Credit card training is not consistently being completed within the required time frames.

Observation:

1 new credit card handler at the Mesa Arts Center (MAC) Box Office in the Arts & Culture department did not complete credit card handling training within 3 months, as required by policy.

2 active credit card handlers in PRCF did not complete the training in calendar years 2019 or 2020 (to date), and 1 new credit card handler did not complete the training at all, much less within the 3 months required.

Criteria:

PCI DSS v3.2.1, Requirements and Security Assessment Procedures, Requirement 12.6.1: "*Educate personnel upon hire and at least annually.*"

Minimum Required Credit Card Handling Procedures, Merchant and Agent Responsibilities, Item #2: "*Agents shall receive training on Handling Procedures within three months of assignment to a position that requires Cardholder Data handling duties, and at least every year thereafter.*"

Comments:

Without training, employees may unknowingly mishandle credit card data, putting customers at risk of credit card fraud. Although the number of employees that were not compliant was minimal, the processes in the departments do not appear to be working to ensure that all credit card handlers are taking required training timely.

Recommendation(s) and Management's Action Plan(s):

Recommendation #2-1: Arts & Culture staff should implement a control to ensure that new credit card handlers complete training within 3 months.

Action Plan #2-1: Implement defined process to ensure that Department of Arts and Culture is providing requisite Cash and Credit Card Training within 3 months. Please see detailed process in the attached Appendix.

Individual or Position Responsible: Marcus Steele, Fiscal Analyst

Estimated Completion Date: New procedure is effective immediately, as of 6-10-20.

Recommendation #2-2: PRCF should implement a control to ensure that all credit card handlers complete training within the required timeframes.

Action Plan #2-2: PRCF IT will forward any request for software access that allows for processing financial transactions to PRCF Finance before setting up the user's access. PRCF Finance will confirm that user has completed required training, cash and credit card handling, and inform PRCF IT that the individual can now be set up to handle financial transactions. PRCF Finance will work with PRCF IT in order to have access to audit users and their primary and secondary user access/permissions.

PRCF keeps a list of credit card handlers which includes when they took their training. On a monthly basis PRCF receives a similar list of card handlers from Financial Services which includes the date of their last training. The Financial Services list is highlighted based on if their training is past due or coming due. PRCF reconciles the list and sends back to Financial Services the list with additions and deletions. PRCF sends an email to the appropriate staff and their supervisor as to their need to take the required training(s). If the training is not taken within the appropriate timeframe, an additional email is sent stating that the card handler is not permitted to handle financial transactions until the training has been completed. The Accounting Specialist that processes deposits will be required to verify that any employees that process financial transactions are up to date on their training(s).

In Observation #2, the employees that had not taken the required training were employees that previously did not have card handling responsibilities or it was reported that they no longer performed those duties, but then had those job duties added or added back at a later date and were given user access by PRCF IT that then allowed them to process financial transactions. The change in duties was not known to PRCF Finance and was a weakness in the controls. The requirement to have PRCF IT confirm with PRCF Finance that the required training has been completed before granting access to processing financial transactions should address the weakness.

Individual or Position Responsible:
Linda Smith and Gayle Malloy

Estimated Completion Date: July 31, 2020

APPENDIX

Department of Arts and Culture

Cash & Credit Card Training Procedures

New city employee training:

1. The supervisor will require the new employee to take the tests online through their city sign-on the first week of employment.

New temp training:

1. Cash and Credit Card training is provided to each new temp by their supervisor as a part of their orientation.
2. After completion of the training, the supervisor sends the completed tests to the Department's Finance team.
3. The Finance team sends the completed Cash & Credit Card Training tests and signed acknowledgements to the City's Department of Finance for their records.
4. The Department of Arts and Culture's Finance team then updates our Cash & Credit Card tracking spreadsheets on SharePoint with their test dates.

Ensuring Staff Receive Training:

1. The City's Finance Office sends the Department of Arts and Culture the City's monthly cash and credit card training reports.
2. The Department of Arts and Culture reviews the report and updates its internal tracking spreadsheets to ensure that our employees' training completion dates are correct. The Department of Arts and Culture maintains a cash and credit card training spreadsheet on its SharePoint site.
3. Based on that training report, the Department of Arts and Culture will notify each supervisor if any of their employees need to complete their initial training. The deadlines for the training will be included in the notice.
4. For retraining of cash and credit card handling, the employee and employee's supervisor will be notified by the Finance team to retake the training 60 days before their current training expires.
5. Each supervisor is required to respond to the Department's Finance team when their staff complete the required training or retraining.
6. Finance staff will then send a notice to the employee, their supervisor, and the deputy director 30 days prior to the date of expiration if the employee has not completed the training, requiring the training be completed within the next two weeks. The supervisor will notify the deputy director and the finance staff when the training has been completed.
7. The Finance staff will call the employee's supervisor and will notify the Director if the employee has not completed the training within that two-week period.
8. If the training is not completed by the deadline, the Finance staff will notify the deputy director and this failure to train staff will be noted in the supervisor's PAF.