MOBILITY DEPARTMENT
PARKING DIVISION
DATA EXCHANGE AUDIT 21-04
January 14, 2021

CITY OF TAMPA

Jane Castor, Mayor **Internal Audit Department**

Christine Glover, Internal Audit Director

January 12, 2021

Honorable Jane Castor
Mayor, City of Tampa
1 City Hall Plaza
Tampa, Florida

RE: Contract No.: HSMV-0417-19 Memorandum of Understanding (MOU) – Data Exchange Audit 21-04

Dear Mayor Castor:

Attached is the Internal Audit Department's report on Mobility Department's Parking Division, Data Exchange Audit 21-04.

The internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of the MOU, and applicable laws and are adequate to protect the personal data from unauthorized access, distribution, use, modification, or disclosure. This includes both policies/procedures in place for personnel to follow and data security procedures/policies in place to protect personal data. Internal Audit certifies that the data security procedures/policies have been approved by a Risk Management IT Security Professional. All deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence.

We thank the aforementioned management and staff for their cooperation and assistance during this audit.

Sincerely,
/s/ Christine Glover

Christine Glover, MS, MBA, CIA, CFE, CGAP
Internal Audit Director

cc: John Bennett, Chief of Staff
Dennis Rogero, Chief Financial Officer
Jean Duncan, Administrator of Infrastructure and Mobility
Gina Grimes, City Attorney
Vik Bhide, Mobility Director
Russell Haupert, Chief Technology Officer
Kelly Stephens, Parking Division Manager

MOBILITY DEPARTMENT
PARKING DIVISION
DATA EXCHANGE AUDIT 21-04

/s/ Anthony Tiwari

Anthony Tiwari MAC, CISA
Auditor

/s/ Christine Glover

Christine Glover, MS, MBA, CIA, CFE, CGAP
Audit Director

/s/ Jane Castor

Honorable Jane Castor
Mayor

MOBILITY DEPARTMENT
PARKING DIVISION
DATA EXCHANGE AUDIT 21-04

BACKGROUND

The Parking Division (Division) of the Mobility Department is responsible for the operation of all City of Tampa (City) public parking. The Division develops parking policy and specific facility expansion plans to serve the parking demand in the central business district and adjacent commercial areas. The Division's processes require an exchange of information; motor vehicle tag information is forwarded to the Florida Department of Highway Safety and Motor Vehicles (FLHSMV) and data is accessed from the Driver and Vehicle Information Database (DAVID).

Pursuant to Section VI., Compliance and Control Measures, Part A, Internal Control and Data Security Audit, of the HSMV-0417-19 Memorandum of Understanding (MOU) between the FLHSMV and the Division, adopted on September 6, 2018, continued access to personal data is contingent upon the Division having appropriate internal controls in place at all times to protect data received from the FLHSMV from unauthorized access, distribution, use, modification or disclosure. A resolution 2018-791 adopted and passed the requirements documented in the MOU.

STATEMENT OF OBJECTIVES

This audit was conducted upon the request from the Management of the Infrastructure and Mobility Department. The objectives of the audit were to assess that:

1. The Division has policy and procedure manuals documenting internal controls relating to prevent unauthorized access, distribution, use, modification, or disclosure of the FLHSMV data received.
2. The data security policies and procedures have been approved by a Risk Management Information Technology (IT) Security Professional.
3. The Transport Layer Security (TLS) version must use 1.2 or higher encryption protocols during transmission of FLHSMV data.
4. All the Division's employees are trained and made aware of information security best practices.
5. Security patches and updates are installed on the Division's computers in a timely manner.
6. A formal information security event reporting policy and procedure must be established.
7. A Disaster Recovery Plan for IT Infrastructure must be established to include the Division's systems that contain violations data.
8. Access to DAVID must be monitored on an ongoing basis to determine that it has been completed by the approved individual for the appropriate purpose.
9. A user access review, including privileged accounts, is consistently performed.
10. Users have the appropriate levels of access to applications in the scope of this review.

STATEMENT OF SCOPE

The audit period covered January 2019 through December 2020. Both qualitative and quantitative assessments were performed to determine whether the management and staff of the Division were fulfilling their stated duties and responsibilities in accordance with Section VI of the MOU. Original records as well as copies were used as evidence and verified through observation and physical examination.

STATEMENT OF METHODOLOGY

We achieved our audit objectives by utilizing the following methods:

1. Conducted interviews with the Division and City’s IT Department (T&I) to gain an understanding of internal controls over data exchange security.
2. Reviewed internal policy and procedures manuals to determine alignment to the standards in the International Organization for Standardization for Information Security Management (ISO 27001).
3. Performed a data reliability analysis to determine completeness and accuracy of system generated information.
4. Examined T&I’s network diagram displaying the location of the Division's systems/applications.
5. Examined the results of the most recent system vulnerability testing performed.
6. Reviewed the results of a risk assessment for identifying, assessing, and monitoring network vulnerabilities.
7. Examined the latest anti-virus protection definitions installed on the Division’s hardware.
8. Reviewed the report of the Division’s employees that completed the required annual information security training.
9. Reviewed the process for applying timely security patches and updates to the Division’s computers.
10. Reviewed the results of the third-party service provider’s assessment with the Payment Card Industry Data Security Standard Requirements and Security Assessment Procedures (PCI DSS).
11. Reviewed the process for granting users access to in-scope applications.

STATEMENT OF AUDITING STANDARDS

We conducted this performance audit 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 findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our conclusions based on our audit objectives.

AUDIT CONCLUSIONS

Based upon the audit work performed, our conclusions are as follows:

1. The Division has policy and procedure manuals documenting internal controls relating to prevent unauthorized access, distribution, use, modification, or disclosure of the data received.
2. The data security policies and procedures have been approved by a Risk Management IT Security Professional.
3. The Transport Layer Security (TLS) version is currently 1.2 encrypted during transmission of FLHSMV data.
4. All the Division's employees are trained and made aware of information security best practices.
5. Security patches and updates are installed by T&I on the Division's computers in a timely manner.
6. A formal information security event reporting policy and procedure is established.
7. A Disaster Recovery Plan for IT Infrastructure is established to include the Division's systems that contain violations data.
8. Access to DAVID is not monitored on an ongoing basis to determine that it has been completed by the approved individual for the appropriate purpose.
9. A review of user access for all users, including privileged accounts, is not consistently performed.
10. Users did not have the appropriate levels of access applications in the scope of this review.

INTERNAL MONITORING

STATEMENT OF CONDITION: A Quarterly Quality Control Review Report of users must be performed in DAVID to determine that unauthorized access or misuse of information contained in the database has not occurred. For the audit period, the Division has not documented the required Quarterly Quality Control Review Report of users.

CRITERIA: According to the MOU Section VI. Compliance and Control Measures, Subsection A. states that a Quarterly Quality Control Review Report must be completed within 10 days after the end of each quarter and maintained for two years.

CAUSE: The Division does not have a documented policy and procedure in place to perform a Quarterly Quality Control Review of the users in DAVID.

EFFECT OF CONDITION: Unauthorized access or misuse of information contained in the system can occur potentially causing loss of access to DAVID.

RECOMMENDATION 1: Division management should work with T&I to develop a policy and procedure to perform and document a Quarterly Quality Control Review Report each quarter to monitor compliance with the MOU. The following must be included in the Quarterly Quality Control Review Report:

1. A comparison of the DAVID users by agency report with the agency user list.
2. A listing of any new or inactivated users since the last quarterly quality control review.
3. Documentation verifying that usage logs has been internally monitored to ensure proper, authorized use and dissemination.

MANAGEMENT RESPONSE: Management agrees with Internal Audits findings and recommendations.

A review of users was performed by the On-Street Supervisor, on 12/29/20. The On-Street Supervisor is the current administrator of DAVID for Parking. All active users accounts were verified to be current Parking Division employees in DAVID. All previous inactive user accounts access was verified as still inactive in DAVID.

Going forward, the On-Street Supervisor will be meeting with the T&I Applications Systems Analyst once a quarter to conduct the required Quarterly Control Review Report of users. They will then report the findings to the Parking Chief of Operations, and the Parking Division Manager. The reports will be then be electronically stored for two years.

Parking will begin working with T&I to develop a Division Standard Operating Procedure (SOP) on the DAVID Quarterly Control Review process. The policy will include the three recommended information areas that Internal Audit has suggested.

TARGET IMPLEMENTATION DATE: Audits will be conducted once a quarter as required in the MOU. These audits will be conducted on a calendar year schedule instead of a fiscal year schedule. The 1st quarter audit for 2021 will be due April 1st.

The Division will need at least 45 days to create, review, and approve a SOP for the Quarterly Quality Control Review Report. This should be ready by February 19, 2021.

PRIVILEGED ACCESS

STATEMENT OF CONDITION: The Division uses T2 Parking Systems (T2), a third-party hosted software application, to manage pay station software, ticketing of parking violations and parking permits. Business process requires, and state law allows, motor vehicle tag data be forwarded and retrieved from the FLHSMV database when a parking violation occurs. T2 does not contain personal driver information, only information related to parking violations and driver status. T2 interfaces with the DAVID through manual and automated processes. It was noted that there are 10 users with privileged administrator access and several generic profiles in T2. Internal Audit further noted that several users listed as active did not log in since 2012 and others were not current employees.

CRITERIA: The City's Information Security Policy states that Information Owners are the department managers that designate the relevant sensitivity classification, the appropriate level of criticality and define which users will be granted access. The policy further states that privileges granted to all workers must be periodically reviewed by Information Owners to ensure that only those with a current need to know presently have access to sensitive data.

CAUSE: The Division is not following the City's Information Security Policy to assign the least privileged access needed to complete a defined job role or performed a user access review of all T2 users. Information Owners have not disabled inactive and non-current employees from the system.

EFFECT OF CONDITION: Administrator accounts have administrative control and can grant or revoke users access to the information stored in the application. Privileged accounts have the highest level of control over systems and data; any unauthorized access to, and modifications from, these accounts can have serious consequences. Generic system accounts, dormant and non-current employees can have unsupervised access to data.

RECOMMENDATION 2: Management should adhere to the City's Information Security Policy to allow for the least privileged access and limit the number of users with Administrative roles. Management should work with the City's IT Department to develop a process to ensure that user's access rights are reviewed at regular intervals. Generic system accounts, dormant and non-current employees should be placed as inactive or removed from T2.

MANAGEMENT RESPONSE: Management agrees with Internal Audits findings and recommendations.

Current process- Oracle sends the Division's T&I Applications Systems Analyst, a security alert email when a Parking Division employee has left the City. The T&I Applications Systems Analyst is responsible for deactivating and activating user accounts for Parking Division applications.

A review of users was performed by the T&I Applications Systems Analyst and the Parking Support Supervisor on 12/29/20. All legacy users (prior to T&I Applications Systems Analyst's tenure) were removed, as well as any dormant Accounting and T&I staff. The Parking On-street Supervisor confirmed status of employees under her purview and are now current. The Parking On-street Coordinator confirmed employees under her purview will be required to login to T2 Flex monthly from now on to ensure current, active status.

Generic System Admin Users were left in place until confirming with T2 Systems Support these are not being used for any back-end tasks. Once confirmed that the generic accounts are not needed, they will be removed from the system.

Future process- T&I Applications Systems Analyst has set up a recurring monthly appointment with the Parking Support Supervisor, to ensure T2 Flex Users are reviewed monthly to double-check and ensure the least number of users have the least access possible. Additionally, each month access levels of all employees will be reviewed to ensure they have the proper access and least privileged access as possible.

TARGET IMPLEMENTATION DATE: Review of all users and access levels is completed and ongoing at this time. The division will implement and follow the City's Information Security policy for user access.