POST AUDIT REPORT
PARKING AND IT
DATA EXCHANGE AUDIT
PAR21-07

November 9, 2021

City of West Palm Beach
Internal Auditor's Office

Beverly Mahaso Esq., CIA, CFE
Chief Internal Auditor

WEST PALM BEACH

Internal Audit

November 9, 2021

Audit Committee
City of West Palm Beach
401 Clematis Street
West Palm Beach, Florida

RE: POST AUDIT REPORT OF PARKING AND IT DATA EXCHANGE (PAR 21-07)

Dear Audit Committee Members:

In FY2020, the Internal Auditor's Office released an audit of Parking and IT Data Exchange. The audit was conducted pursuant to a requirement within a Memorandum of Understanding (MOU) between the City and the State. We conducted a follow up review to determine the status of the recommendations that were identified. We performed certain procedures, as enumerated below, with respect to activities of the Parking Department and the IT Department in order to render a conclusion on the status of the recommendations made as a result of that review.

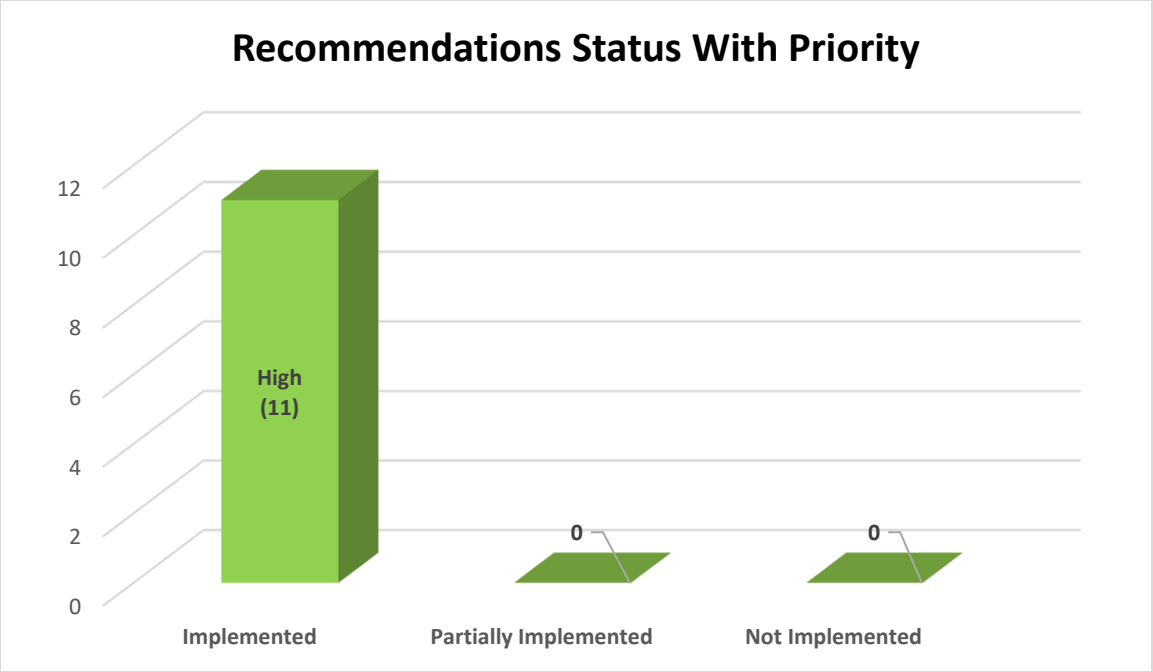
This Post Audit Report (PAR) consisted primarily of inquiries of City personnel and examinations and analyses of various supporting documentation and data. It was substantially less in scope than an audit in accordance with generally accepted government auditing standards.

The evidence obtained provided a reasonable basis for our conclusions; however, had an audit been performed, other matters might have come to our attention that would have been reported to you and our conclusions may have been modified.

The audit contained eleven (11) recommendations that addressed the audit's findings. Based on the review performed, we concluded that all recommendations were implemented. There were three minor observations that represent opportunities for improvement, however, they did not rise to the level of a deficiency.

As such, we concluded that the Parking and IT Departments met the requirements of the MOU. All deficiencies/issues found during the audit have been corrected and measures have been put in place to prevent recurrence.

We have enclosed a table listing all the recommendations with the current statuses. We found that management made significant efforts to take corrective action.



We thank the personnel from the Parking and IT Departments for their assistance in conducting this review and on continuing implementation efforts.

Respectfully Submitted,

s/ Beverly Mahaso
Chief Internal Auditor

cc:

Joseph Peduzzi, Commission President
Christina Lambert, Commissioner
Shalonda Warren, Commissioner
Christy Fox, Commissioner
Kelly Shoaf, Commissioner
Keith James, Mayor
Faye Johnson, City Administrator
Edward Davis, Parking Systems Administrator
Paul Jones, Chief Information Officer

Encl.

Legend
- Implemented
- Partially Implemented
- Not Implemented

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

AUDIT RECOMMENDATIONS

No.	Auditor's Condition and Recommendation	Management's Initial Response	Auditor's Status Update
1 High Priority	**Condition:** **Lack of Required Policies and Procedures** During the audit period of August 14, 2018 – May 31, 2020, the IT Department was not able to provide formal policies and procedures governing 9 IT security processes identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy. We noted the following policies are not currently in place as required: • Data Security - Data Classification and Date Disposal • Physical Security • Firewall and Outside Network Segmentation • Security Patching • Application Service Provider - regarding the vetting process for 3rd party vendors to ensure security controls are in place and align with the City of West Palm Beach standards • Acceptable Encryption - Data At-Rest Encryption Standards • Malware/Virus Protection • Security Monitoring and	**Management's Initial Response:** We agree with the finding above. The City's leadership has made cyber security a number one priority, as made evident by the recent addition of a CIO and a Security Officer, both of whom are highly credentialed and have strong security backgrounds. It is fully recognized and understood that security policies and procedures are a critical element of any security program, and we have recently begun an engagement with a third party to assist in the development and implementation of all the missing documentation. As part of this process, all required documentation, including appropriate compliance measures, are scheduled to be developed and fully deployed by the end of August 2021. **Target Implementation Date:** August 1, 2021	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF OCTOBER 2021** As part of the remediation process, Internal Audit inquired and obtained the policies governing the following areas: • Data Security • Passwords • Acceptable Encryption • Access Control • Account Management for User Accounts • Application Service Provider • Incident Handling • Security Monitoring and Auditing • Network Interconnectivity • Malware/Virus Protection Per inspection of the policies provided above, Internal Audit noted no observations of deficiencies within the control testing and the controls were able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy.

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

Legend
- Implemented
- Partially Implemented
- Not Implemented

	Auditing • Passwords **Recommendation:** The IT Department should ensure all relevant IT Security policies are established to reflect the current procedures and are periodically updated to consider new laws and regulations, as well as changes within the organization. Further, training should be provided and documented to ensure staff awareness and consistent compliance. Having policies and procedures in place helps ensure that the City will meet standards across the board.		
2 High Priority	**Condition:** **Lack of Third-Party Security Assessments** Third-Party application service providers typically obtain an independent assessment of their controls and security protocols to ensure compliance with security standards and identify weaknesses if applicable. This is known as a SOC report that the third-party provides to a client in order to provide assurances that the third-party's security protocol meets the client's requirements. During the audit period (August 14,	**Management's Initial Response:** Agree. **Target Implementation Date:** January 31, 2021	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF OCTOBER 2021** As part of the remediation testing, Internal Audit obtained and inspected the Department's 2021 policy governing Third Party Service Providers. Per inspection of the Cloud Based Computing Policy and per inquiry with IT Security, City staff met with the IPS vendor to ensure that all standards outlined within the Cloud Based Computing Policy were compliant.

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

	2018 – May 31, 2020), the Parking Department was unable to provide the SOC report for the third-party application service provider, Integrated Parking System (IPS). Therefore, we were not able to determine whether the required security topics around General Security, Network Security, Host Security, and Web Security were tested by an independent 3rd party and whether or not they met security requirements. The Department is required to know whether or not security requirements are met, typically through an independent assessment before obtaining the software and periodically thereafter. However, we found that the Parking Department did not perform a review/assessment of the vendor's security prior to the implementation of the IPS system to determine if the IPS vendor's security controls align with the City's standards and requirements nor did the Department have periodic independent testing results provided by the vendor. Based on the above, we concluded that the following areas failed due to not having independent testing to		Additionally, it was noted that the Departments obtained the 2021 SOC report from the 3rd party vendor. Internal Audit deemed this remediation to be sufficient and to meet the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy. **Minor Observation:** The Departments should have evidence to support that they reviewed the report and were satisfied with the control environment provided by the 3rd Party vendor.

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

	verify security standards prior to or during the use of the IPS software: • Backups, • Change Management/Security Patching, and • Security Monitoring and Auditing. **Recommendation:** It is recommended that the Parking Department request that the IPS vendor provide a SOC Report to ensure alignment with the City and the Florida External IT Security Policy standards. This report should be provided periodically, typically at a yearly frequency.		
3 High Priority	**Condition:** **Improper Termination of Users** During the audit period, we noted the following observations, for the sample of terminated users related to the Parking Department and the IPS application: • One of the sampled users did not have an IT ticket submitted for access to be removed. • All 5 of the sampled users did not have tickets created on or before their termination date for their network access to be removed.	**Management's Initial Response:** IT Management is aware of a gap in policies to increase awareness specifically related to sensitive or confidential data, and such policies, along with procedures, are in development as a mechanism to strengthen the security posture of the City and protect the City's users and its citizens. IT Management also wants to emphasize that access to the FTP server is restricted to System Administrators. Employees cannot access the data on that server with	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF OCTOBER 2021** As part of our remediation testing, Internal Audit inquired with IT Security and inspected the newly created Logical Security and IT General Security Policies, to obtain an understanding of how full-time employees and contractors are removed from the system upon the employee's termination. Additionally, Internal Audit performed sample testing of terminated employees and contractors, after the target

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

	• 2 of the 5 sampled users did not have access removed from their privileged account within the IPS application. • 1 of the 5 sampled users had an IT ticket request for termination created 14 days after access was already removed. • When performing testing over the City's Security Awareness Training, 1 sampled active IPS user was noted as a terminated employee since 2005. **Recommendation:** The Parking and IT Departments should ensure that access is appropriate at all times including terminations. Thus, we recommend that termination requests are completed on or before a user's termination date. In addition, access should be removed and/or disabled within the next business day of the user's termination date for the in-scope systems. Specific to the IPS application, we recommend that a thorough periodic user access review be performed to determine if other terminated users exist and remove any duplicate or inappropriate users.	or without an Active Directory account. A security application monitors the FTP Server and emails monthly reports, allowing management to verify access to secure locations was legitimate. As mentioned, IT Management is developing policies and procedures to ensure access to applications is removed when an employee ends employment with the City. Parking Administration agrees with the recommendation and is in the process of developing policies and procedures to ensure that access to the application is terminated when an employee is no longer with the City. We also had a user report created to audit and track active users and their access levels. **Target Implementation Date:** January 31, 2021	implementation date; noting that the terminated samples were appropriately removed. Per inspection of the evidence provided and the testing performed, Internal Audit noted no observations of deficiencies within the control testing. As such the control was able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy. **Minor Observation:** The Departments should have evidence to clearly state the date that access was removed. However, we note that the terminated users that were tested did not have access at the time of the review.

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

Legend
- Implemented
- Partially Implemented
- Not Implemented

4 High Priority	**Condition:** **Lack of Patching Procedures** During the audit period, per inquiry with management, it was noted that there is no formal policy or standard regarding frequency of security and patch updates. Thus, a patching process does not currently exist. **Recommendation:** To the extent relevant, IT should ensure that patches are applied throughout the IT environment in a timely manner. Internal Audit noted that 2020 security updates and patches were applied to the in-scope server that was installed on June 3, 2020. However, it is recommended that the IT Department create and implement a patching process to ensure that the in-scope server continues to be patched when new security updates are available	**Management's Initial Response:** IT Management agrees with the recommendation that patches are applied to an environment in a timely manner. IT has been developing a comprehensive, formalized Patch Management procedure that is applicable to all servers and services, not just the single FTP server utilized for the Data Exchange. In terms of development and testing, as mentioned in the 'Criteria' section, IT Management disagrees with a need for that level of separation for this particular server. Due to the server functioning solely as a Secure FTP holding point to allow file exchanges between the Florida HSMV and Integrated Parking Systems, it does not require the same level of testing before patches as an application or infrastructure system would require. This server would suffice with IT Staff performing proactive measures such as a VMWare Snapshot or Rubrik Backup prior to	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF OCTOBER 2021** As part of our remediation testing, Internal Audit performed inquiry with IT Security to obtain an understanding of the newly implemented patching protocols. Internal Audit obtained the newly created Server Patch Management Policy and the accompanying Monthly Patch flow chart. Additionally, Internal Audit obtained the latest Windows Patch applied and the relevant ticketed evidence. Per inspection of the evidence provided, Internal Audit noted no observations of deficiencies within the control testing, and the control was able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy.

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

		applying security patches, and if the FTP software experienced an issue, utilizing a "rollback" procedure if necessary. A "rollback" is a much more efficient and timely method for handling an issue due to a patch than any possible means for testing the Secure FTP connections. **Target Implementation Date:** December 31, 2020	
5 High Priority	**Condition:** **Inadequate Encryption and Secure File Transfer** During the audit period, it was noted that at-rest encryption is not enabled for the FTP Server. In addition, we noted that a server using an FTP connection was used until July 2020, which indicates a secure connection was not used to transfer data. We do note that as of July 2020, a SFTP connection is now being used to exchange data which is a secure connection. **Recommendation:** We recommend that the IT Department enable at-rest encryption for the in-scope server.	**Management's Initial Response:** IT Management agrees that the system should have encryption-at-rest. The initial steps to employ this are currently in motion. IT Management wants to emphasize that although the data on the server contains PII under Florida Law by a combination of name with address or driver's license number and protecting this data is a high priority, the data does not contain Social Security Information or Credit Card Information. IT Management wants to note that only the vendors have access to their FTP accounts and connect via Secure FTP (encrypted) as per the	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF OCTOBER 2021** As part of the remediation process, Internal Audit obtained the newly created Acceptable Encryption Policy and the Information Technology General Security Policy. Internal Audit noted that the policies mention specific cipher requirements, as well as encryption standards. Internal Audit obtained documents evidencing that the FTP server utilizes AES 128 encryption protocol for the data-at-rest and met best-practice requirements.

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

Legend
- Implemented
- Partially Implemented
- Not Implemented

		MOU. The server is not accessible by regular users using Windows logon credentials with the exception of IT Administrators. **Target Implementation Date:** December 31, 2020	Additionally, Internal Audit inspected the 2021 SOC report for data hosted by the vendor and did not note any deviations. Per inspection of the evidence provided, Internal Audit noted no observations of deficiencies within the control testing and the control was able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy.
6 High Priority	**Condition:** **Lack of Separation of Environments** During the audit period of August 14, 2018 thru May 31, 2020, it was noted that a dedicated QA, Development, and/or Test environment did not exist for the CWPB FTP Server which does not meet the Florida DHSMV External IT Security Policy requirements. Due to no separation of environments, security patches are unable to be tested prior to implementation to the production environment. In addition, backup restoration procedures are unable to be tested to ensure files and data can be recovered within a QA environment. **Recommendation:** The IT Department should create a test environment for the CWPB FTP	**Management's Initial Response:** The new IT leadership team immediately recognized the need for a segregated QA/Testing and development environment and is currently in the process of implementing this environment. However, the system that is being audited is only used as a file repository and not an application server, so we feel the risk of implementing patches on this system is minimal. **Target Implementation Date:** July 1, 2021	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF OCTOBER 2021** As part of the remediation testing, Internal Audit inquired with IT Security regarding testing environments. Additionally, Internal Audit was able to obtain evidence that IT utilizes a segregated testing environment. Per inspection of the evidence provided, Internal Audit noted no observations of deficiencies within the control testing, and the control was able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy.

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

Legend
- Implemented
- Partially Implemented
- Not Implemented

	Server to ensure patches and backups are tested appropriately prior to deployment.		
7 High Priority	**Condition:** **Insufficient Password Requirements** During the audit period of August 14, 2018 thru May 31, 2020, the password parameters for the City's FTP Server and the Integrated Parking System (IPS) did not meet the Florida DHSMV External IT Security Policy requirements. City FTP Server - password expiration setting of 180 days, and password history of 5 passwords remembered; does not meet the Florida DHSMV External IT Security Policy requirement of passwords expiring every 90 days and 10 passwords remembered. IPS Application – the password character length of 6 characters does not meet the Florida DHSMV External IT Security Policy requirement of 8 characters. **Recommendation:**	**Management's Initial Response:** **IT Department:** We will adjust the password parameters for the CWPB FTP Server and the Integrated Parking System (IPS) to adhere to the requirements referenced below. Password Setting Requirements: Expiration - 90 days Character Length - 8 Character Complexity Enabled - to include a combination of alpha (upper and lower case), numeric, and special characters (unless a particular system does not allow) Password History - 10 Lockout Threshold – 5 **Target Implementation Date:** August 21, 2020 **Parking Department** - Agree **Target Implementation Date:** Dependent on IPS, the provider, but no later than January 31, 2021.	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF OCTOBER 2021** Internal Audit obtained documentation evidencing the password parameters for both in-scope systems: City FTP Server and the IPS application. Per inspection of the evidence provided, Internal Audit noted no observations of deficiencies within the control testing and the control was able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy.

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

	The IT Department should ensure that passwords are configured appropriately and meet required standards and/or regulations as follows: • For the City's FTP Server, it is recommended that the IT Department ensure that the password parameters align with the Florida External IT Security Policy. • For the IPS application, it is recommended that the Parking Department contact the IPS vendor and ensure password settings align with the Florida External IT Security Policy.		
8 High Priority	**Condition:** **Insufficient Knowledge of Users and Permissions** At the time the audit was conducted, knowledge of the IPS permissions that allow access to read sensitive data (e.g., personally identifiable information) was unknown to the IPS owners and administrators in the Parking Department, though this is important information that they should be aware of. We found that the Parking Department was not aware of	**Management's Initial Response:** Agree. **Target Implementation Date:** January 31, 2021	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF OCTOBER 2021** As part of the remediation testing, Internal Audit made inquiries of IT Security personnel regarding their knowledge of permissions and tasks found within the IPS application. As requested by the Departments, the IPS vendor provided the Departments with a listing of all the permission names and the respective definitions. Using this knowledge, IT and the IPS business

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

	some users or their permissions. We reviewed the users and confirmed that the users were valid, and the access was appropriate, however, this is information that the Department should be aware of. **Recommendation:** The Parking Department should ensure that it is fully aware of permissions granted to users by obtaining an understanding of the purpose for each permission within the IPS application from the vendor and ensuring that the users with access to sensitive data are appropriate. Once a full understanding is acquired, the Department should ensure that it requests the appropriate permissions for users and subsequently verifies the access granted by the IPS vendor.		owner, created a role-based approach for all IPS access, and any unnecessary access was purged. Per inquiry with the Departments and per inspection of the evidence provided, Internal Audit noted no observations of deficiencies within the control testing, and the control was able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy.
9 High Priority	**Condition:** **Insufficient Provisioning Access Requests** At the time the audit was conducted, we were provided with e-mail evidence to add a sampled user to IPS. However, there was no mention of what access should be granted for this user. Therefore, this provisioning	**Management's Initial Response:** Agree. **Target Implementation Date:** January 31, 2021	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF OCTOBER 2021** As part of our remediation testing, Internal Audit performed an inquiry with IT Security, and inspected the newly created Logical Security and IT General Security Policies, to obtain an understanding of how newly hired full-

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

	request did not meet the access request standards. **Recommendation:** The Parking Department should ensure all access requests are fully documented, to include the specific permissions requested and follow up to confirm that the access granted matches the request.		time employees and contractors are provisioned with system access. Additionally, Internal Audit performed sample testing of newly hired employees and contractors, after the Department's target implementation date; and noted that the new hires, with active access, had appropriate documentation prior to granting them access and that the level of access was also appropriate. Per inspection of the evidence provided and the testing performed, Internal Audit noted no observations of deficiencies within the control testing. As such the control was able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy.
10 High Priority	**Condition:** **Lack of User Access Reviews** At the time the audit was conducted, it was noted that there is currently no process to periodically review access to the in-scope systems by either the Parking Department or the IT Department. For example, Internal Audit noted terminated users with current access to the IPS application, including an officer who was terminated in 2005.	**Management's Initial Response:** IT Management agrees with the finding and is in the early stages of developing a process to conduct user access and user account reviews. As the process develops, we will determine a reasonable schedule for each department to perform these reviews with appropriate compliance documentation. Parking Department – Agree.	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF October 2021** As part of the remediation process, Internal Audit inquired with IT Security and inspected the WPB's Logical Access Policy, to gain an understanding of the annual access review of the IPS application. Internal Audit obtained the documentation for the latest Access Review conducted in May 2021, and

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

	Recommendation: The IT and Parking Departments should implement a periodic user access review process to ensure that the users with access to the in-scope systems are: a) active employees of the City and b) that access is appropriate for the user's job function.	**Target Implementation Date:** January 31, 2021	inspected the documentation evidencing that the IPS Annual Access Review was conducted accurately and completely, and was thoroughly documented. Per inspection of the evidence provided and the testing performed, Internal Audit noted no observations of deficiencies within the control testing. As such the control was able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy.
11 High Priority	**Condition:** **Lack of User Training** During the audit, we found that the Parking Department did not provide training to users related to 1. the confidentiality of the information accessible by them, and 2. civil and criminal sanctions specified in State and Federal laws. This training as well as acknowledgements of understanding are required under the MOU. **Recommendation:** The Parking Department should ensure that users with access to the information are fully trained and aware of the sensitive nature of the data that they have access to as well as the civil and criminal sanctions, by	**Management's Initial Response:** Agree. **Target Implementation Date:** January 31, 2021	**AUDITOR'S STATUS UPDATE: IMPLEMENTED** **UPDATE AS OF October 2021** As part of the remediation process, Internal Audit inquired with IT Security, regarding training for users that have access to IPS (which contains PI and PII data). Internal Audit obtained and inspected the training materials, noting that Cyber Security and other IT Security related content is discussed. Additionally, as this training is mandatory, Internal Audit performed testing of all active IPS users to verify that users underwent the appropriate training. Internal Audit obtained signed acknowledgment forms evidencing that

POST AUDIT REPORT
PARKING AND IT DATA EXCHANGE

	conducting training when users are first granted access, then subsequently providing the training annually. Users must sign acknowledgement forms specifically indicating their understanding of the confidentiality of the information and specifically acknowledging their understanding of the civil and criminal sanctions for misuse.		all users received the access policy and that they were acknowledging that they understood the policy. Per inspection of the evidence provided, Internal Audit noted no exceptions within the control testing, and was able to satisfy the criteria identified within the Memorandum of Understanding (MOU) and the Florida DHSMV External IT Security Policy. **Minor Observation:** The Departments should ensure that the supporting documentation clearly states when the training was provided.