OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

John A. Carey
Inspector General

Inspector General
Accredited

"Enhancing Public Trust in Government"

Redacted per 282.318(5)(6)(8), F.S.

Audit Report

2021-A-0005

Town of Palm Beach Internal Control and Data Security

May 27, 2021

OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

AUDIT REPORT
2021-A-0005

DATE ISSUED: MAY 27, 2021

John A. Carey
Inspector General

Inspector General
Accredited

"Enhancing Public Trust in Government"

TOWN OF PALM BEACH INTERNAL CONTROL AND DATA SECURITY

SUMMARY

WHAT WE DID

We conducted an internal control and data security audit of the Town of Palm Beach (Town). This audit was based on the Town's request and was performed as part of the Office of Inspector General, Palm Beach County (OIG) 2021 Annual Audit Plan.

Our audit focused on internal controls and data security activities for motor vehicle information obtained through the Town's Memorandum of Understanding (MOU) HSMV-0216-20 with the Florida Department of Highway Safety and Motor Vehicles (HSMV) from January 21, 2020 through April 30, 2021.

WHAT WE FOUND

We found the Town had generally adequate controls for:

- Segregation of duties;
- Physical security of computers and IT equipment;
- Logical access controls and passwords;
- Security breaches and incidents;
- Malware and virus protection; and
- Detecting misuse of information and monitoring information use.

We found control weaknesses related to the Town's compliance with MOU requirements and data security for the motor vehicle information.

[redacted]
The Town [redacted]

Instruction and User Acknowledgement Forms

We reviewed the Town's records to determine if the 22 personnel that had access to motor vehicle information from HSMV were appropriately instructed by the Town and acknowledged their understanding regarding the confidential nature of the motor vehicle information and the civil and criminal sanctions for unauthorized use, as required under the MOU. We found:

- Eight (8) personnel that had access to the motor vehicle information from HSMV for over a year before

[1] The AIMS system is the parking management system utilized by the Town and is used to prepare billing notices for parking tickets.

the Town provided the proper instruction.
- Ten (10) personnel had access to the motor vehicle information from HSMV for over a year prior to signing the Town's acknowledgment form.

A lack of knowledge related to the confidentiality of the information and the civil and criminal sanctions for unauthorized access, use, or disclosure of the information increases the risk of improper handling and unauthorized use of such information.

Annual Review of User Accounts and Access

The Town did not perform the annual review of user accounts and access, as required by its Office of Information Technology (OIT) Technologies Policy.

A lack of monitoring and review of user accounts and access increases the risk of unauthorized access to the motor vehicle information obtained from HSMV and the Town's systems.

Notification for Change in Technical Contact

The Town did not notify the HSMV of a change in the Technical Contact within five (5) business days, as required by the MOU.

Failing to comply with the requirements of the MOU could result in termination of the MOU by the HSMV.

Corrective Action

During the audit, the Town provided the Acknowledgment forms for the three (3) Police Department Parking Enforcement personnel and performed the user account and access reviews and provided the completed verification forms showing that all users with access to the HSMV data were authorized.

WHAT WE RECOMMEND

Our report contains four (4) findings and offers seven (7) recommendations. Implementation of the recommendations will 1) assist the Town in strengthening internal controls and data security, and 2) help ensure compliance with the MOU and related requirements.

The Town has taken corrective actions to implement the recommendations.

We have included the Town's management response as Attachment 1.

BACKGROUND

The Town was originally created under the general laws of the State of Florida on April 17, 1911. The municipality continued to operate and function under the special and general laws of Florida until a Charter was granted by Chapter 7683, Special Acts, Laws of Florida, 1917, whereby a new municipality was created. The current Charter became effective on February 9, 2000. The Town is located on a barrier island in the eastern part of Palm Beach County.

The Town has a Mayor and five (5) Council members who are elected for two (2) year terms. The Town Council has all powers, legislative and judicial. The executive powers of the Town are vested in the Mayor, the Town Council, and the Town Manager. The Mayor shall be elected at large by the electors of the Town for a two (2) year term. The Mayor shall be recognized as the head of the Town government for all ceremonial purposes, for service of process, execution of contracts, deeds, and other documents, and as the Town official designated to represent the Town in all agreements, but shall have no administrative duties. The Mayor does not have voting powers, but does have the power to veto any ordinance or resolution adopted by the Council.

The Town Manager is the chief administrative officer of the Town. The Town Manager is responsible to the Town Council for the administration of the day-to-day activities of the Town and for all Town officers and employees. The 2020 population was estimated to be 8,409 plus an estimated 15,000 additional seasonal residents (November to May).

MOU

According to the MOU for Driver's License and/or Motor Vehicle Record Data Exchange, Contract Number HSMV-0216-20 between the Town and the HSMV, effective February 5, 2020, HSMV agrees to provide electronic access to motor vehicle information to the Town. The data obtained is used by the Finance Department to obtain registered vehicle owner information for billing/notices for parking tickets. The MOU term is for three (3) years.

The MOU is contingent upon the Town having appropriate internal controls in place at all times to ensure that the data provided is protected from unauthorized access, distribution, use, modification, or disclosure. To ensure that this requirement is met, the MOU requires the Town to submit to HSMV an Internal Control and Data Security Audit on or before the first anniversary of the execution date of the MOU and an Annual Certification Statement within fifteen (15) business days after each anniversary for the duration of the MOU. The HSMV granted the Town an extension until May 31, 2021 to submit the Internal Control and Data Security Audit.

The OIG 2021 Annual Audit Plan included Management Requests. The Town requested that the OIG perform an Internal Control and Data Security Audit of the Town, as provided

by the MOU for Driver's License and/or Motor Vehicle Record Data Exchange Contract Number HSMV-0216-20.

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objectives of the audit were to determine if:

- Controls were adequate for the MOU activities and information usage,
- Activities were adequately documented, approved, and monitored, and
- Activities using the computer system were in compliance with requirements.

The scope of the audit included, but was not limited to, internal control and data security activities for driver license and motor vehicle information obtained through the Town's MOU with HSMV from January 21, 2020[2] through April 30, 2021.

The audit methodology included, but was not limited to:

- Completion of data reliability and integrity assessment of related computer systems;
- Review of regulatory guidance, policies and procedures, and related requirements;
- Review of records and reports;
- Review of the HSMV-0216-20 MOU;
- Completion of process walk-throughs;
- Review of data security and related activity controls;
- Interview of appropriate personnel; and
- Detailed testing of activities related to driver license and motor vehicle information.

As part of the audit, we completed a data reliability and integrity assessment for the computer systems used by the Town for motor vehicle activities. We determined that the computer-processed data contained in the AIMS computer system[3] and FTP data exchange system[4] were sufficiently reliable for purposes of the audit.

We conducted this 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 findings and conclusions based on our audit objectives.

[2] The MOU was dated January 21, 2020 with an effective date of February 5, 2020. The scope of the audit began with the signed MOU, in order to review activities related to entering into the MOU.

[3] The AIMS system is the parking management system utilized by the Town and is used to prepare billing notices for parking tickets.

[4] The FTP (file transfer protocol) data exchange system is the system utilized by the Town to obtain vehicle registered owner information from the HSMV.

FINDINGS AND RECOMMENDATIONS

Finding (1): The Town [redacted], as required by the MOU.

The MOU states,

> **IV. Statement of Work**
>
> …
>
> **B**. The Requesting Party agrees to:
>
> …
>
> 7. Protect and maintain the confidentiality and security of the data received from the Providing Agency in accordance with this MOU and applicable state and federal laws.
>
> **V. Safeguarding Information**
>
> …
>
> The Parties mutually agree to the following:
>
> …
>
> **C.** Information obtained from the Providing Agency will be stored in a location that is physically and logically secure from access by unauthorized persons.
>
> …
>
> **D.** The requesting Party shall develop security requirements and standards consistent with Section 282.318, Florida Statutes, Florida Administrative Code Rule 74-2, and the Providing Agency's security policies; and employ adequate security measures to protect Providing Agency's information, applications, data, resources, and services. The applicable Providing Agency security policies are set forth in Attachment III.
>
> …
>
> **E.** Access to the information received from the Providing Agency will be protected in such a way that unauthorized persons cannot view, retrieve, or print the information.

The Florida Highway Safety and Motor Vehicle (FHSMV) External Information Security Policy[5] states,

> **#A-02: Data Security**
>
> …

[5] The HSMV requires external parties using its systems to comply with the HSMV External Information Security Policy.

> **4.0 Data Storage or Transmission**
> All users who are responsible for the secure storage or transmission of the Department's data must do so only in conformance with this policy. Where confidentiality, privacy or sensitivity requires, **stored or transmitted data must be secured via Department-approved encryption technology.** This does not supersede provisions of the Public Records Act that states, "computer records are public records," but serves to protect data while stored. [Emphasis added]
>
> …
>
> **#B-01: Acceptable Encryption**
>
> …
>
> **4.0 Policy**
> Encryption is the primary means for providing confidentiality for information that can be stored or transmitted, either physically or logically… Information resources that stores or transmits sensitive or confidential data must have the capability to encrypt information.

The motor vehicle information obtained from HSMV through the FTP data exchange is used to update the registered owner information for parking tickets in the AIMS system for billing purposes.

The AIMS system parking ticket database is automatically updated for the current registered owner information weekly based on the motor vehicle information obtained from HSMV that corresponds to the vehicle tag number on the parking ticket.

[redacted]

[redacted]

[redacted]

The Town [redacted], as required by the MOU and HSMV External Information Security Policy. Failing to comply with the requirements of the MOU could result in a finding by HSMV of non-compliance, the imposition of remedies under the MOU, suspension of the MOU, the need for a Corrective Action Plan, and/or termination of the MOU by the HSMV.

Additionally, [redacted]

Recommendations:

(1) The Town [redacted]

(2) The Town [redacted]

Management Responses:

(1) The Town [redacted]

(2) The Town [redacted]

Finding (2): The Town did not provide the required instruction and maintain user acknowledgment forms in a current status for all personnel with access to confidential information, as required by the MOU.

The MOU states,

> **V. Safeguarding Information**
>
> …
>
> The Parties mutually agree to the following:
>
> …
>
> **F.** All personnel with access to the information exchanged under the terms of this MOU will be instructed of, and acknowledge their understanding of, the confidential nature of the information. These acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency within ten (10) business days of a request.
>
> **G.** All personnel with access to the information will be instructed of and acknowledge their understanding of the civil and criminal sanctions specified in state and Federal Law for unauthorized use of the data. These acknowledgements must be maintained in a current status by the Requesting Party and provided to the Providing Agency within ten (10) business days of a request.

The Town created an acknowledgment form for personnel with access to the motor vehicle information to confirm that they were informed on the confidential nature of information and the civil and criminal sanctions for unauthorized use.

We compared the acknowledgement forms signed by personnel and training records provided by the Town to the MOU start date of February 5, 2020 and the users with access to the motor vehicle information provided by the HSMV under the MOU to determine if the Town provided the required instruction regarding the confidentiality of the information and the civil and criminal sanctions for unauthorized use of the information and maintained user acknowledgment forms in a current status for all personnel with access to motor vehicle information, as required by the MOU.

We reviewed the Town's records to determine if the 22 personnel that had access to motor vehicle information from HSMV were appropriately instructed by the Town and acknowledged their understanding regarding the confidential nature of the motor vehicle information and the civil and criminal sanctions for unauthorized use, as required under the MOU. We found:

- The Town did not instruct one (1) Police Department Parking Enforcement Officer and seven (7) Finance Department personnel with access to the motor vehicle information via the AIMS system until February 2021 and March 2021, respectively. The Parking Enforcement Officer and Finance personnel had access to the information for over a year prior to receiving the required instruction.
- The Town did not obtain acknowledgment forms for seven (7) Finance Department personnel with access to the motor vehicle information via the AIMS system until March 2021. The Finance personnel had access to the information for over a year prior to acknowledging their understanding as required under the MOU.
- The Town did not obtain acknowledgment forms for three (3) Police Department Parking Enforcement personnel with access to the motor vehicle information via the AIMS system. The Parking Enforcement personnel had access to the information for over a year prior to acknowledging their understanding as required under the MOU.

It appears the Finance Director was unaware of the MOU requirements.

The Town personnel that had access to motor vehicle information exchanged under the MOU may not have been aware of the confidentiality of the information and the civil and criminal sanctions for unauthorized use of the information, as required by the MOU.

The Town did not maintain in a current status user acknowledgment forms for all personnel with access to the motor vehicle information exchanged under the MOU, as required by the MOU.

Failing to comply with the requirements of the MOU could result in a finding by HSMV of non-compliance, the imposition of remedies under the MOU, suspension of the MOU, the need for a Corrective Action Plan, and/ or termination of the MOU by the HSMV.

Additionally, a lack of knowledge related to the confidentiality of the information and the civil and criminal sanctions for unauthorized use of the information increases the risk of improper handling and unauthorized use of such information.

Corrective Action

The Town provided the Acknowledgment forms for the three (3) Police Department Parking Enforcement personnel during the audit.

Recommendations:

(3) Upon approval of access, the Town instruct personnel regarding the confidentiality of the motor vehicle information exchanged under the MOU and the civil and criminal sanctions for unauthorized use of that information and obtain the personnel's signed acknowledgement forms confirming their understanding.

(4) The Town obtain signed acknowledgment forms for the three (3) Police Department Parking Enforcement personnel.

Management Response:

All new employees will be trained and sign acknowledgment forms prior to using the AIMS system. The Police Department Parking Enforcement personnel have been certified by FDLE and in addition, they have signed the acknowledgment forms for the AIMS system.

Finding (3): The Town did not complete the annual review of user accounts and access, as required by the Town's IT Technologies Policy.

The Town's Office of Information Technology (OIT) Technologies Policy states,

> *Chapter One – Security*
>
> Section One – Passwords & User Management
>
> …
>
> 1.5.4 Annually
>
> …
>
> User accounts for the Active Directory are reviewed and every Department is notified of all employee access capabilities. Each Department will then notify the Office of Information Technology of any changes that are needed regarding access to systems and software. This report will be signed off by each Department Director.
>
> …
>
> *Appendix – Agreements & Verifications*
>
> *Attachment E*
>
> Town of Palm Beach

Information Technology Active User Account Verification
Attachment to the Information Technologies Policy
Effective Date: November 1, 2020

In order to assure that all of the user accounts that have access to the Town of Palm Beach computer systems are active and legitimate, each Department Director is required to review the attached report of users within their department that have active computer accounts.

The report lists the names of the users with an account. The Department Director must verify that the names are active employees and make any changes to the report.

This form verifies that the Department Director has reviewed this report, made that appropriate changes and returned the corrected report to the Information Technology Manager.

…

Attachment F

Town of Palm Beach
Information Technology User Access and Authority Verification
Attachment to the Information Technologies Policy
Effective Date: November 1, 2020

In order to assure that all of the user accounts that have access to the Town of Palm Beach computer systems are setup correctly and have the appropriate access to the Town's computer software, the Department Director is required to review the attached report of users and their access to the Town's software systems.

The report lists the names of the users with an account and the software systems that they have access to, along with the authorities within that system. The Department Director must verify that the names are active employees and that the access and authorities are correct.

Make any changes necessary to the report.

This form verifies that the Department Director has reviewed this report, made that appropriate changes and returned the corrected report to the Information Technology Manager.

We requested the Information Technology Active User Account Verification forms and Information Technology User Access and Authority Verification forms (verification forms) completed since the MOU went into effect[6] for the Town's departments with personnel that had access to the motor vehicle data obtained from HSMV. We requested the

[6] The MOU was effective on February 5, 2020.

verification forms to verify that the annual reviews of user accounts and access were being performed, as required by the OIT Technologies Policy, and to verify that all users with access to the HSMV data were authorized. The Town's Interim IT Director could not locate any forms completed during that time frame.

The Town's Interim IT Director did not provide a reason why the Town did not perform the annual reviews. It appears the annual reviews should have been performed under the former IT Director's tenure.

The Town did not comply with its OIT Technologies Policy.

A lack of monitoring and review of user accounts and access increases the risk of unauthorized access to the motor vehicle information obtained from HSMV and the Town's systems.

Corrective Action

During the audit, the Town performed the user account and access reviews and provided the completed verification forms showing that all users with access to the HSMV data were active, legitimate users with the appropriate level of access.

Recommendations:

(5) The Town perform and document an annual user account and access review, as required by the OIT Technologies Policy.

(6) The Town perform and document the user account and access reviews annually going forward, as required by the OIT Technologies Policy.

Management Response:

IT is notified by HR of all employee terminations and at that time they inactivate the user on the active directory which should ensure no terminated employees have improper access. In addition, IT will conduct an annual review of user account and access as required by the OIT Technologies Policy.

Finding (4): The Town did not notify the HSMV of a change in the Technical Contact within five (5) business days, as required by the MOU.

The MOU states,

> **IV. Statement of Work**
>
> …
>
> **B**. The Requesting Party agrees to:
>
> …
>
> 14. Notify the Providing Agency within five (5) business days of any changes to the name, address, telephone number and/or email address of the Requesting Party, its Point-of-Contact for Consumer Complaints, and/or its Technical Contact. The information shall be

emailed to DataListingUnit@flhsmv.gov. Failure to update this information as required may adversely affect the timely receipt of information from the Providing Agency.

During an interview with the Town's Assistant Finance Director and Interim IT Director on April 8, 2021, we inquired whether there had been any changes to the MOU point-of-contacts. They confirmed that the only change was for the Technical Contact that had been the former IT Director, who separated employment with the Town on March 24, 2021. The Town stated the Technical Contact was currently the Interim IT Director and that they had not notified the HSMV of the change in the Technical Contact.

On the same day subsequent to our interview with the Town, the Town's Finance Director notified the HSMV of the change in the Technical Contact. Based on the separation date of the former IT Director, the Town should have notified the HSMV of the change in Technical Contact by April 1, 2021.

It appears the Town was not aware of the MOU requirement to notify the HSMV within five (5) business days of a change in the Technical Contact. As a result, the Town did not notify the HSMV regarding the change in the Technical Contact within five (5) business days, as required by the MOU.

Failing to comply with the requirements of the MOU could result in a finding by HSMV of non-compliance, the imposition of remedies under the MOU or law, suspension of the MOU, the need for a Corrective Action Plan, and/ or termination of the MOU by the HSMV. Additionally, the failure to update the Technical Contact within five (5) business days, as required, could adversely affect the Town's timely receipt of information from HSMV.

Recommendation:

(7) The Town notify the HSMV of any future changes to the name, address, telephone number, and/or email address of the Requesting Party, its Point-of-Contact for Consumer Complaints, and/or its Technical Contact within five (5) business days.

Management Response:

The Town will ensure that when a change is made to the contacts, we will notify HSMV in a timely manner.

ACKNOWLEDGEMENT

The Inspector General's audit staff would like to extend our appreciation to the Town of Palm Beach's staff for their assistance and support in the completion of this audit.

This report is available on the OIG website at: http://www.pbcgov.com/OIG. Please address inquiries regarding this report to the Director of Audit by email at inspector@pbcgov.org or by telephone at (561) 233-2350.

ATTACHMENT

Attachment 1 – Town of Palm Beach's Management Response

ATTACHMENT 1

TOWN OF PALM BEACH'S MANAGEMENT RESPONSE

TOWN OF PALM BEACH

Town Manager

May 7, 2021

Ms. Hillary Bojan
Office of Inspector General
P.O. Box 16568
West Palm Beach, FL 33416-6568

Re: Management Response to Town of Palm Beach Internal Control and Data Security Audit 2021-A-0005

Dear Ms. Bojan:

Below are the Town of Palm Beach's responses to the findings for the above referenced audit. The Town accepts the recommendations and is taking the following corrective action to resolve these issues.

Finding 1. The Town [redacted], as required by the MOU.

Recommendation 1. The Town [redacted]

Management Response: [redacted]

Recommendation 2. The [redacted]

Management Response: The Town [redacted]

Post Office Box 2029 • 360 South County Road • Palm Beach, Florida 33480
Telephone (561) 838-5444 • Facsimile (561) 838-5417
E-mail: finance@townofpalmbeach.com • Website: www.townofpalmbeach.com

Finding 2. The Town did not provide the required instruction and maintain user acknowledgment forms in a current status for all personnel with access to confidential information, as required by the MOU.

Recommendation 3. Upon approval of access, the Town instruct personnel regarding the confidentiality of the motor vehicle information exchanged under the MOU and the civil and criminal sanctions for unauthorized use of that information and obtain the personnel's signed acknowledgement forms confirming their understanding.

Recommendation 4. The Town obtain signed acknowledgment forms for the three Police Department Parking Enforcement personnel.

Management Response: All new employees will be trained and sign acknowledgment forms prior to using the AIMS system. The Police Department Parking Enforcement personnel have been certified by FDLE and in addition, they have signed the acknowledgement forms for the AIMS system.

Finding 3: The Town did not complete the annual review of user accounts and access, as required by the Town's IT Technologies Policy.

Recommendation 5. The Town perform and document an annual user account and access review, as required by the OIT Technologies Policy.

Recommendation 6. The Town perform and document the user account and access reviews annually going forward, as required by the OIT Technologies Policy.

Management Response: IT is notified by HR of all employee terminations and at that time they inactivate the user on the active directory which should ensure no terminated employees have improper access. In addition, IT will conduct an annual review of user account and access as required by the OIT Technologies Policy.

Finding 4: The Town did not notify the HSMV of a change in the Technical Contact within five business days, as required by the MOU.

Recommendation 7. The Town notify the HSMV of any future changes to the name, address, telephone number, and/or email address of the Requesting Party, its Point-of-contact for Consumer Complaints, and/or its Technical Contact within five business days.

Management Response: The Town will ensure that when a change is made to the contacts, we will notify HSMV in a timely manner.

Sincerely,

Kirk Blouin,
Town Manager

Cc: John Carey, Inspector General

Post Office Box 2029 • 360 South County Road • Palm Beach, Florida 33480
Telephone (561) 838-5444 • Facsimile (561) 838-5417
E-mail: finance@townofpalmbeach.com • Website: www.townofpalmbeach.com