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), F.S.

Audit Report

2020-A-0001

Town of Palm Beach Internal Controls and Data Security

October 11, 2019

John A. Carey
Inspector General

OFFICE OF INSPECTOR GENERAL
PALM BEACH COUNTY

AUDIT REPORT
2020-A-0001

DATE ISSUED: OCTOBER XX, 2019

Inspector General
Accredited

"Enhancing Public Trust in Government"

TOWN OF PALM BEACH – INTERNAL CONTROLS AND DATA SECURITY

SUMMARY

WHAT WE DID

We conducted an internal controls 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) 2020 Annual Audit Plan.

Our audit focused on internal controls and data security activities for driver license and motor vehicle information obtained through the Town's Memorandum of Understanding (MOU) HSMV-0151-19 with the Florida Department of Highway Safety and Motor Vehicles (HSMV) from September 20, 2018 through September 30, 2019.

WHAT WE FOUND

We found the Town had generally adequate controls for:

- Segregation of duties,
- Physical security of computers and IT equipment,
- Security breaches and incidents,
- Records retention,
- Malware and virus protection, and
- Detecting misuse of information and monitoring information use.

We found control weaknesses for the Town's internal controls and data security related to driver license and motor vehicle information.

Access

[redacted]

Additionally, [redacted]

Passwords

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

The Town's [redacted]

The Town [redacted]

[redacted]

[redacted]

Account Management

The Town [redacted]

Training

The Town staff [redacted]

WHAT WE RECOMMEND

Our report contains seven (7) findings and offers twenty-two (22) 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 2018 population was approximately 8,802, plus as 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-0151-19 between the Town and the HSMV, effective October 15, 2018, HSMV agrees to provide electronic access to driver license and motor vehicle information to the Town. The data obtained is used by the Town's Risk Management Department to ensure compliance with Chapter 322, Florida Statutes and the Town's Authorized Driver Policy. 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 OIG 2020 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-0151-19.

OBJECTIVES, SCOPE, AND METHODOLOGY

The overall objectives of the audit were to determine if:

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

The scope of the audit included, but was not limited to, internal controls and data security activities for driver license and motor vehicle information obtained through the Town's MOU with HSMV from September 20, 2018[1] through September 30, 2019.

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-0151-19 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 driver license and motor vehicle activities. We determined that the computer-processed data contained in the Eden computer system was sufficiently reliable for purposes of the audit. The information from the FTP data exchange system was not sufficiently reliable for purpose of this audit because all users shared the same credentials.

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.

[1] The MOU was signed on September 20, 2018 with an effective date of October 15, 2018. The scope of the audit began with the signed MOU, in order to review activities related to entering into the MOU.

FINDINGS AND RECOMMENDATIONS

Finding (1): [redacted]

The MOU states,

> **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...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 3.
>
> ...
>
> **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 (HSMV) External Information Security Policy[2] states,

> **#A-04: Passwords**
>
> ...
>
> **2.0 Policy and Standards**
>
> ...
>
> 4. Passwords and user names shall not be shared with anyone to include co-workers or contractors. Passwords must be treated as confidential information. Credentials (UserID and passwords) are for exclusive use only by the user to which they are assigned.
>
> ...

[2] The HSMV requires external parties using its systems to comply with the HSMV External Information Security Policy, which is Attachment III of the MOU.

12. Passwords must be encrypted during transmission and storage using appropriate encryption technology.

...

13. Passwords should not be written down and stored at your workstation in your office.

...

#B-02: Access Control

...

2.0 Policy

...

1. Each user accessing a Department information resource shall be assigned a unique personal identifier, commonly referred to as either a user account, Logon ID, user identification, or User ID.

2. Users shall not under any circumstances use another user's account logon or credentials.

3. User access rights shall be established based on approved written requests. The user identification shall be traceable to the user for the lifetime of the records or reports in which they appear.

...

#B-03: Account Management for User Accounts

...

3.0 Policy

...

1. All accounts created must have an associated request and approval that is appropriate for the Department's information resource or service.

This MOU requires the Town to have appropriate internal controls in place to ensure that the data is protected from unauthorized access, distribution, use, modification, or disclosure.

The Town's OIT Technologies Policy states,

Chapter One – Security

Section One – Passwords & User Management

...

1.1.1 User Passwords

...

Employees shall consider computer passwords as confidential material. [redacted]

1.1.2 Sharing Passwords

...

User identifications (ID's) and passwords shall not be used by anyone other than the original user to whom the ID and password were assigned. If a user's ID and password are being used by another employee, the password will immediately be changed, and written notification will be sent to that user's [redacted]

We found that [redacted]

Additionally, we noted that the password was not properly secured or encrypted, and the [redacted] The default password was never changed, and all users [redacted]

We determined that [redacted]

At the time of the audit, the Town [redacted]

The IT department was not aware that [redacted] and stated that no new users had been setup recently.

The Town did not [redacted], which is in violation of the MOU terms and may lead to termination of the MOU.

[3] Driver license and motor vehicle information is considered personal and confidential information according to Section 119.0712(2)(b), Florida Statutes.

[4] FTP is defined by the MOU as batch/file transfer protocol and refers to the electronic transfer of data in a secure environment.

The Town did not [redacted]

[redacted]

Additionally, [redacted] increases the risk that unauthorized persons may obtain access to the State computer system and obtain and disseminate personal and confidential data in a manner not authorized by the law and the MOU.

Corrective Action

[redacted]

Recommendations:

(1) The Town [redacted]

(2) The Town establish individual user accounts and passwords for each authorized user of the FTP data exchange.

(3) The Town [redacted]

(4) The Town ensure [redacted]

(5) The Town [redacted] **to only the employees who need to have access to perform their regular job duties and assignments.**

(6) The Town perform and document a review of user access to the FTP data exchange and any locations containing driver license and motor vehicle information, at a minimum once per year.

Management Response:

(1) The Town will immediately comply with this recommendation.

(2) The Town has established individual user accounts for users needing access to the FTP data exchange for the HSMV data.

(3) The Town [redacted]

(4) The Town [redacted]

(5) The Town limited access to the authorized employees.

(6) The Town IT Technology Policy updated to incorporate annual user audit.

Finding (2): The Town [redacted]

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's [redacted] to the personal and confidential information.

The [redacted] the Town violated the MOU terms, which may lead to termination of the MOU.

Additionally, [redacted] 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

[redacted]

Recommendations:

(7) The Town [redacted]

(8) The Town train all employees [redacted]

(9) The Town [redacted]

Management Response:

(7) [redacted]

(8) Risk has trained all [redacted] **Staff who have access.**

(9) [redacted]

Finding (3): [redacted]

The MOU states,

> **VI. Compliance and Control Measures**
>
> **A. Internal Control and Data Security Audit**
>
> ...
>
> The audit shall indicate that the internal controls governing the use and dissemination of personal data have been evaluated in light of the requirements of this 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. The audit shall certify that the data security procedures/policies have been approved by a Risk Management IT Security Professional.

The Town's [redacted] for compliance with the MOU requirements. The [redacted] which was approximately [redacted] to the commencement of the MOU on [redacted]

[redacted] with the MOU requirements, which may lead to termination of the MOU.

Additionally, the [redacted]

Corrective Action [redacted]

Recommendation:

(10) The Town perform and document a review of the Town's [redacted] **and any other related policies and procedures** [redacted]

[redacted] **to identify and resolve any inconsistencies with the MOU.**

Management Response:

(10) The [redacted] has reviewed the updated [redacted] policy.

Finding (4): Audit trails and logs are not sufficient, maintained, and reviewed, as required by the MOU.

The MOU states,

> **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...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 3.
>
> ...
>
> **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 HSMV External Information Security Policy[2] states,

> **#A-02: Data Security**
>
> ...
>
> **6.0 Management Responsibilities**
> Network operations and systems administration personnel shall ensure that adequate logs and audit trails are maintained. Logs and audit trails must at a minimum record access to data, records, and activation of industry recognized security mechanism for protection of confidential and sensitive data.
>
> ...

#B-20: Security Monitoring and Auditing

...

3.0 Policy

...

2. Monitoring consists of activities such as the periodic review of

...

e. Application logs

Additionally, the Town's OIT Technologies Policy states,

Chapter One – Security

...

Section Five – Security Audit Procedures

...

1.5.1 Weekly

...

Email logs from both internal and external systems are reviewed. The logs are examined for several items including but not limited to spamming, misuse, overuse, intrusion and errors. These logs are reviewed [redacted]

Web browsing logs are scanned for key words to determine misuse. Event logs for both internal and external web servers are reviewed for access violations. Web pages are also reviewed to make sure that they have not been tampered with.

FTP (File Transfer Protocol) logs are reviewed for both access violations as well as errors. Directories exposed to FTP usage are also examined.

...

Active Directory logs are reviewed as needed and all system activity is monitored daily.

[redacted] job logs are reviewed as needed and all system activity including security violations are monitored automatically.

Backup logs are reviewed.

...

1.5.2 Monthly

...

Network access is reviewed and the firewall configuration and logs are checked.

...

Network Servers are restarted and file structures are reviewed for any misuse and errors. Internet systems are especially examined for intrusion and viruses.

The Town's [redacted]

The Town [redacted]

[redacted]

[redacted]

[redacted]

Corrective Action

[redacted]

Recommendations:

(11) The Town [redacted]

(12) The Town [redacted]

(13) The Town [redacted]

Management Response:

(11) The Town [redacted]

(12) The Town [redacted]

(13) The Town [redacted]

Finding (5): The Town [redacted]

The MOU states,

> **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...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 3.
>
> ...
>
> **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 HSMV External Information Security Policy[2] states:

#A-02: Data Security

...

7.0 Data Classification

...

External Entities are required to abide by data classification requirements as outlined by the Department. Data classification shall be done in accordance with Federal Information Processing Standards (FIPS) Publication 199 and is necessary to enable the allocation of resources for the protection of data assets, as well as determining the potential loss or damage from the corruption, loss, or disclosure of data. To ensure the security and integrity of all data, any data asset is Public, Sensitive or Confidential and should be labeled accordingly.

All data falls into one of the following categories:

- Public:
  Information or data that is not classified as sensitive or confidential. Information that, if disclosed outside the State or agency, would not harm the State or Department, its employees, customers, or business partners. This data may be made generally available without specific data custodian approval.

- Sensitive:
  Information not approved for general circulation outside the State or Department where its loss would inconvenience the State/Department or management but disclosure is unlikely to result in financial loss or serious damage to credibility. Examples would include internal memos, minutes of meetings, and internal project reports. Security at this level is controlled but normal.

- Confidential:
  - Data that, by its nature, is exempt from disclosure under the requirements of Chapter 119, F.S.
  - Data whose loss, corruption, or unauthorized disclosure would be a violation of federal or State laws/regulations. Information of a proprietary nature. Procedures, operational work routines, project plans, designs, or specifications that define the way in which the organization operates.
  - Data whose loss, corruption, or unauthorized disclosure would tend to impair business functions or result in any business, financial, or legal loss.
  - Data that involves issues of personal credibility, reputation, or other issues of privacy.

- Highly sensitive internal documents that could seriously damage the State or Department if such information were lost or made public. Information usually has very restricted distribution and must be protected at all times.

The Town's [redacted]

[redacted]

Corrective Action

[redacted]

Recommendations:

(14) The Town [redacted]

(15) The Town [redacted]

Management Response:

(14) The Town [redacted]

(15) The Town [redacted]

Finding (6): The Town's [redacted]

The MOU states,

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...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 3.

...

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 HSMV External Information Security Policy[2] states,

...

#A-04: Passwords

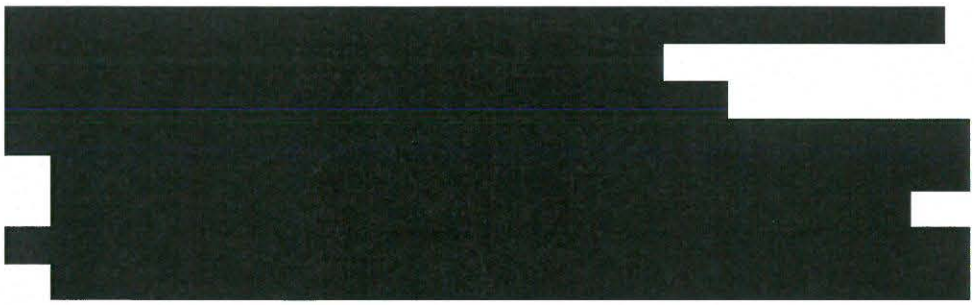
...

2.0 Policy and Standards

...

Passwords, which are the first line of defense for the protection of the Departments information resources, shall be treated as confidential information and must not be divulged.

1. All user accounts used to access the Department information resources shall have passwords of sufficient strength and complexity, and be implemented based on system requirements and constraints, and in accordance with the following rules to ensure strong passwords are established:



[redacted]

2. [redacted]
3. [redacted]
4. [redacted]
5. All users are responsible for the work performed under their credentials (User Id and password). Allowing other users to use your computer while you are logged on is strictly prohibited. [redacted]

[redacted]

6. [redacted]
7. [redacted]
8. [redacted]
9. [redacted]
10. [redacted]
11. [redacted]

12. [redacted]

13. [redacted]

14. [redacted]

15. [redacted]

16. [redacted]

The Town's OIT Technologies Policy states,

Chapter One – Security

Section One – Passwords & User Management

...

1.1.1 User Passwords

...

[redacted]

Employees shall consider computer passwords as confidential material. As such, written passwords shall not be kept in unsecured areas such as desk tops, desk drawers, etc. [redacted]

...

1.1.2 Sharing Passwords

...

[redacted]

...

1.1.3 Unattended Computers

All computers must be locked or logged off whenever they are unattended. Unattended is defined as being out of the sight and immediate control of the user. As part of this policy, the domain controller will automatically lock a workstation after 30 minutes of inactivity.

Passwords

The Town's [redacted]

Our audit examined the Town's [redacted]

Password Encryption

[redacted]

[redacted]

Unattended Computers

The Town's [redacted]

During interviews, [redacted] Actual operations are in compliance with the MOU requirements.

The Town's [redacted] Additionally, the Town [redacted]

The Town [redacted] Additionally, the Town's [redacted]

[redacted]

Corrective Action

[redacted]

Recommendations:

(16) The Town [redacted]

(17) The Town [redacted]

(18) The Town [redacted]

Management Response:

(16) The Town [redacted]

(17) The Town [redacted]

(18) The Town [redacted]

Finding (7): The Town [redacted]

The MOU states,

> **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...and the Providing Agency's security policies; and employee 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 3.
>
> ...
>
> **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 HSMV External Information Security Policy[2] states,

> **#B-03: Account Management for User Accounts**
>
> ...
>
> **3.0 Policy**
>
> ...
>
> 2. [redacted]
>
> ...

6. [redacted]

7. [redacted]

The Town [redacted]

During an interview, [redacted]

The Town [redacted]

The [redacted]

Corrective Action

[redacted]

Recommendations:

(19) The Town [redacted]

(20) The Town [redacted]

[5] PartnerNet Portal is a web application provided to subscribers to one or more data exchanges provided by the HSMV.

(21) The Town [redacted]

(22) The Town [redacted]

Management Response:

(19) The Town [redacted]

(20) [redacted]

(21) The Town [redacted]

(22) The Town [redacted]

ATTACHMENT

Attachment 1 – Town of Palm Beach's Management Response, page 26-29

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 Director of Audit, by email at inspector@pbcgov.org or by telephone at (561) 233-2350.

ATTACHMENT 1 – TOWN OF PALM BEACH'S MANAGEMENT RESPONSE

TOWN OF PALM BEACH

Office of the Town Manager

October 9, 2019

Ms. Megan Gaillard
Director of Audit
Office of Inspector General
P.O. Box 16568
West Palm Beach, Florida 33416-6568

RE: Management Response to Town of Palm Beach Internal Control and Data Security Audit – HSMV-0151-19 Agreement

Dear Ms. Gaillard,

This is the Town of Palm Beach's response to the findings for Audit completed that focused on internal control and data security relative to the Town's access pursuant to the HSMV-0151-19 agreement. The Town accepts with the 22 recommendations and is taking the following corrective action to resolve these recommendations.

Finding 1. [redacted]

Recommenation 1. The Town [redacted]
Response: The Town will immediately comply with this recommendation.

Recommenation 2. The Town establish individual user accounts and passwords for each authorized user of the FTP data exchange.
Response: Town has established individual user accounts for users needing access to the FTP data exchange for the HSMV data.

Recommenation 3. The Town [redacted]
Response: Town [redacted]

Recommenation 4. The Town [redacted]
Response: [redacted]

Recommenation 5. The Town [redacted] to only the employees who need to have access to perform their regular job duties and assignments.
Response: Town limited access to the authorized employees.

Post Office Box 2029 • 100 South County Road • Palm Beach, Florida 33480
Telephone (561) 838-5410 • Facsimile (561) 838-5411
E-mail: townmanager@townofpalmbeach.com • Website: www.townofpalmbeach.com

Recommenation 6. The Town perform and document a review of user access to the FTP data exchange and any folders containing driver license and motor vehicle information, at a minimum once per year.
Response: Town IT Technology Policy updated to incorporate annual user audit.

Finding 2. [redacted]

Recommenation 7. The [redacted]
Response: [redacted]

Recommenation 8. The Town train all employees [redacted]
Response: Risk has trained all [redacted] staff who have access.

Recommenation 9. The Town [redacted]
Response: [redacted]

Finding 3. [redacted]

Recommenation 10. The Town perform and document a review of the Town's [redacted] and any other related policies and procedures [redacted] to identify and resolve any inconsistencies with the MOU.
Response: The [redacted] has reviewed the updated [redacted] policy.

Finding 4. Audit trails and logs are not sufficient, maintained, and reviewed, as required by the MOU.

Recommenation 11. The Town [redacted]
Response: Town [redacted]

Recommenation 12. The Town [redacted]
Response: Town [redacted]

Recommenation 13. The Town [redacted]
Response: Town [redacted]

Finding 5. The Town [redacted]

Recommenation 14. [redacted]

Response: Town [redacted]

Recommenation 15. The Town [redacted]

Response:Town [redacted]

Finding 6. The Town's [redacted]

Recommenation 16. The Town [redacted]

Response: Town [redacted]

Recommenation 17. The Town [redacted]
Response: Town [redacted]

Recommenation 18. The Town [redacted]

Response:Town [redacted]

Finding 7. The Town [redacted]

Recommenation 19. The Town [redacted]

Response: Town [redacted]

Recommenation 20. The Town [redacted]

Response: [redacted]

Recommenation 21. The Town [redacted]

Response: Town [redacted]

Recommenation 22. The Town [redacted]

Response: Town [redacted]

Sincerely,

Kirk Blouin
Town Manager

C: John Carey, Inspector General