PARKING AND IT DATA EXCHANGE AUDIT AUD20-02

September 8, 2020

City of West Palm Beach Internal Auditor's Office

Beverly Mahaso Esq., CIA, CFE
Chief Internal Auditor

INTENTIONALLY LEFT BLANK

Executive Summary

PARKING AND IT DATA EXCHANGE AUDIT
AUD20-02
September 8, 2020

WEST PALM BEACH
Internal Audit

OVERVIEW

- The Parking Department utilizes data provided by the Florida Department of Highway Safety and Motor Vehicles to identify or confirm driver information as related to parking infractions.
- Data provided is confidential, thus the City and State entered into an MOU which has requirements to ensure the physical and logical security of the information. These requirements include, but are not limited to, inactivation of terminated users, acknowledgements of the confidentiality of information including criminal sanctions for confidentiality violations, professional use of the information, and periodic audits of user activity. As such, this audit was conducted as required in the MOU and necessarily included the IT Department.

SUMMARY FINDINGS

1. **Lack of Policies and Procedures:** The IT Department did not have policies and procedures for 9 IT Security processes as required in the MOU and applicable regulations.
2. **Lack of Third-Party Security Assessments:** The Parking Department did not perform a review of the application service provider's (IPS) security protocol to ensure that it met required standards. As such, three areas failed due to not conducting independent testing.
3. **Improper Termination of Users:** We found several areas of improper termination of users where sampled users were not terminated appropriately across different platforms.
4. **Lack of Patching Procedures:** A patching process did not exist and there were no related policies or procedures.
5. **Inadequate Encryption and Secure File Transfer:** At-rest encryption for the relevant server was not performed and a server using an FTP connection was used until July 2020 which indicates that a secure connection was not used.
6. **Lack of Separation of Environments:** A dedicated test environment did not exist for the server. Due to no separation of environments, security patches cannot be tested prior to implementation.
7. **Insufficient Password Requirements:** The password parameters for the City's server and IPS did not meet regulations.
8. **Insufficient Knowledge of Users and Permissions:** The Parking Department was not aware of some of the IPS users and their permissions.
9. **Insufficient Provisioning Access Requests:** Documentation to add a user to IPS did not state what access should be granted for the user.
10. **Lack of User Access Reviews:** Neither department had a process to periodically review access to the systems.
11. **Lack of User Training:** The Parking Department did not provide training to users regarding the confidentiality of information and the civil and criminal sanctions for misuse.

SUMMARY RECOMMENDATIONS

1. The IT Department should ensure all relevant security policies and procedures are established. Training should also be provided to users.
2. The Parking Department should obtain the SOC report from IPS and ensure that it meets security requirements. In the future, the Departments should perform thorough reviews of third-party service providers to ensure that they align with required security standards.
3. The Departments should ensure that termination requests are completed on or before the user's termination date.
4. The IT Department should ensure that patches are applied throughout the entire IT environment.
5. The IT Department should enable at-rest encryption for the server.
6. The IT Department should create a test environment for the server to ensure patches and backups are tested prior to deployment.
7. The Departments should ensure that passwords configured for the City's server and the IPS application are appropriate and meet regulations. This may require contacting IPS and requesting changes.
8. The Parking Department should be fully aware of all users and obtain an understanding of all user permissions to ensure that access is appropriate.
9. The Parking Department should ensure that all access requests are fully documented to include specific permissions for users and verification of actual access granted.
10. The Departments should implement periodic user access reviews to ensure that users are active employees and access is appropriate.
11. The Parking Department should provide training to users to ensure awareness of sensitive information and legal ramifications. Training should include user acknowledgement of understanding.

INTENTIONALLY LEFT BLANK

Internal Auditor's Office
P.O. Box 3366
West Palm Beach, Florida 33402
Tel: 561-822-1380
Fax: 561-822-1424

September 8, 2020

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

RE: Parking and IT Data Exchange Audit, AUD20-02

Dear Audit Committee Members:

Attached is the City of West Palm Beach's Internal Auditor's Office report on the Parking and Information Technology Data Exchange Audit. This audit was conducted in compliance with a Memorandum of Understanding between the City and the State that required an internal control and data security audit. Certain disclosures and representations in the body of this report have been made based on the requirements and the work performed.

We thank our contracted auditors, Focal Point, for their work in completing this audit. We also thank the management and staff of the Parking Department and the Information Technology Department for their time, assistance, and cooperation during this audit.

Respectfully Submitted,

s/ Beverly Mahaso
Chief Internal Auditor

cc: Keith James, Mayor
Faye Johnson, City Administrator
Ricardo Mendez-Saldivia, Assistant City Administrator
Edward Davis, Parking Administrator
Paul Jones, Chief Information Officer

Contents

Background

The City's Parking Department utilizes data provided by the Florida Department of Highway Safety and Motor Vehicles (DHSMV) to identify or confirm driver information as related to parking infractions. In order to utilize the data provided, the City and DHSMV entered into a Memorandum of Understanding (MOU) to obtain access to the Driver's License and Motor Vehicle Record Data Exchange, which provides remote electronic access to driver license and motor vehicle information. City employees do not have direct access to the database, rather, data is exchanged through a series of scheduled batch jobs that are sent to/from the City's server; and to/from the Integrated Parking System (IPS) application and the Florida DHSMV server. IPS is an application service provider that allows City employees to obtain or enter certain sensitive information when issuing a parking citation. The scheduled batch jobs that occur on a weekly basis, transfer this sensitive information to the City's server, and then from the City's server to the Florida DHSMV server.

Data provided through the data exchange is confidential, thus the MOU has requirements to ensure the physical and logical security of the information. These requirements include, but are not limited to, deactivation of terminated users, acknowledgements of the confidentiality of information including criminal sanctions for confidentiality violations, professional use of the information, periodic reviews and periodic audits of user activity.

This audit was conducted specifically to evaluate the internal controls related to access and usage of the Driver's License and Motor Vehicle Record Data Exchange in accordance with the MOU. We note that while the Parking Department is the primary user of the data, the IT Department is essential in ensuring that required IT security protocols are consistently followed. As such, this audit necessarily included the IT Department.

Statement of Scope

The scope of the audit was from August 14, 2018 to May 31, 2020 (audit period). The audit included tests and reviews of systems, policies, procedures, and processes. Other procedures and reviews outside the audit period were conducted as deemed necessary.

Statement of Objectives

The objectives of this audit were to:

A. Determine whether the internal controls governing the Parking Department's access and usage of the Driver's License and Motor Vehicle Record Data Exchange provided by DHSMV complied with the requirements in the Memorandum of Understanding.
B. Determine whether there were any additional opportunities for improvement.

Statement of Methodology

The methodologies used to meet the audit objectives included the following:

- Conducting interviews and inquiries of personnel in the Parking and IT Departments;
- Reviews of relevant agreements, State laws, and internal policies and procedures;
- Evaluating and testing internal controls as related to applicable systems; and
- Other audit procedures deemed necessary.

Areas under review included but were not limited to user access, data backup, user administration, continuity of operations, incident management, change management, data interfaces, monitoring, and security of information.

Statement of Auditing Standards

We conducted this audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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.

Audit Conclusions and Summary of Findings

The following statements are made in response to disclosure requirements within the MOU.

The Internal Auditor's Office has evaluated the internal controls governing the use and dissemination of personal data based on the requirements in the MOU and applicable laws. We conclude that the Parking and IT Departments did not meet the requirements in the MOU during the audit period. Further, this audit cannot certify that data security procedures/policies have been approved by a Risk Management IT Professional because the majority of the required policies and procedures have not been created. While significant corrective action was actively being taken to resolve the issues identified, this audit cannot certify that all deficiencies/issues found during the audit have been corrected and measures enacted to prevent recurrence. However, this audit can and does indicate that corrective action is being taken expeditiously. The following is a summary of opportunities for improvement that will assist the departments in meeting the requirements in the MOU and applicable laws:

- All required policies and procedures should be drafted, reviewed and implemented and staff trained on them.
- Third-Party vendors should provide their security reports for review by the

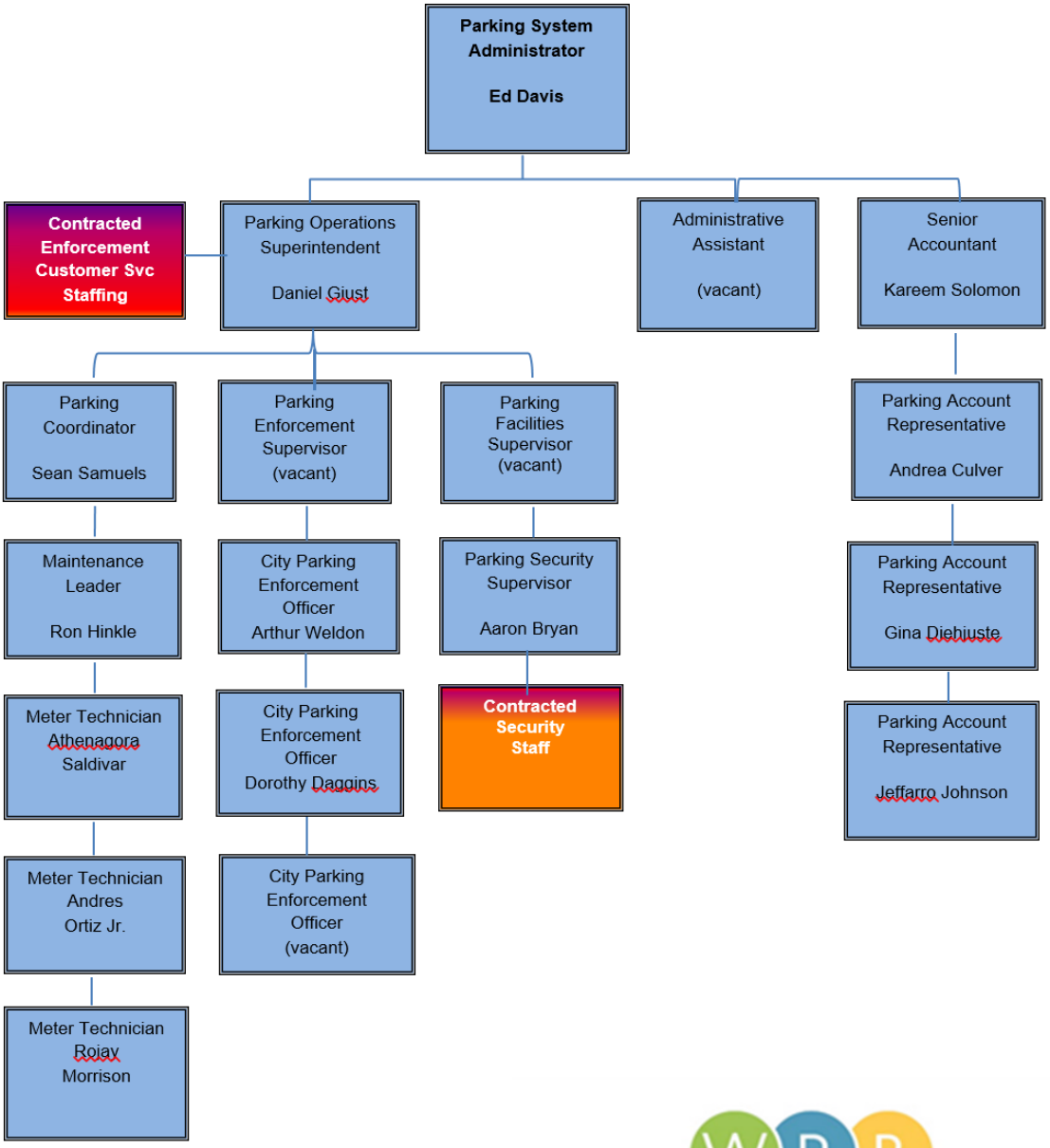
Departments and IT prior to use and periodically thereafter.

- Adequate monitoring of users should be in place to include ensuring that requests for access are sufficient and appropriate, actual access granted is appropriate, system use is monitored, and user access is terminated timely.
- Systems should be patched timely.
- Appropriate encryption and secure file transfers should be in place.
- Separate testing/quality assurance environments should be available and utilized prior to deployment of changes.
- Password settings should meet requirements and standards throughout the various systems.
- Management should be knowledgeable of users and associated permissions to ensure appropriate access.
- Management should ensure that users receive all necessary training periodically.

Noteworthy Accomplishments

We found knowledgeable and dedicated employees that were receptive to our recommendations for improvement. Specifically, we found that both the Parking Department and the IT Department were proactive in taking corrective action. In some instances, corrective action was taken within days of the issues being identified. We commend the departments on their efforts at continuous improvement.

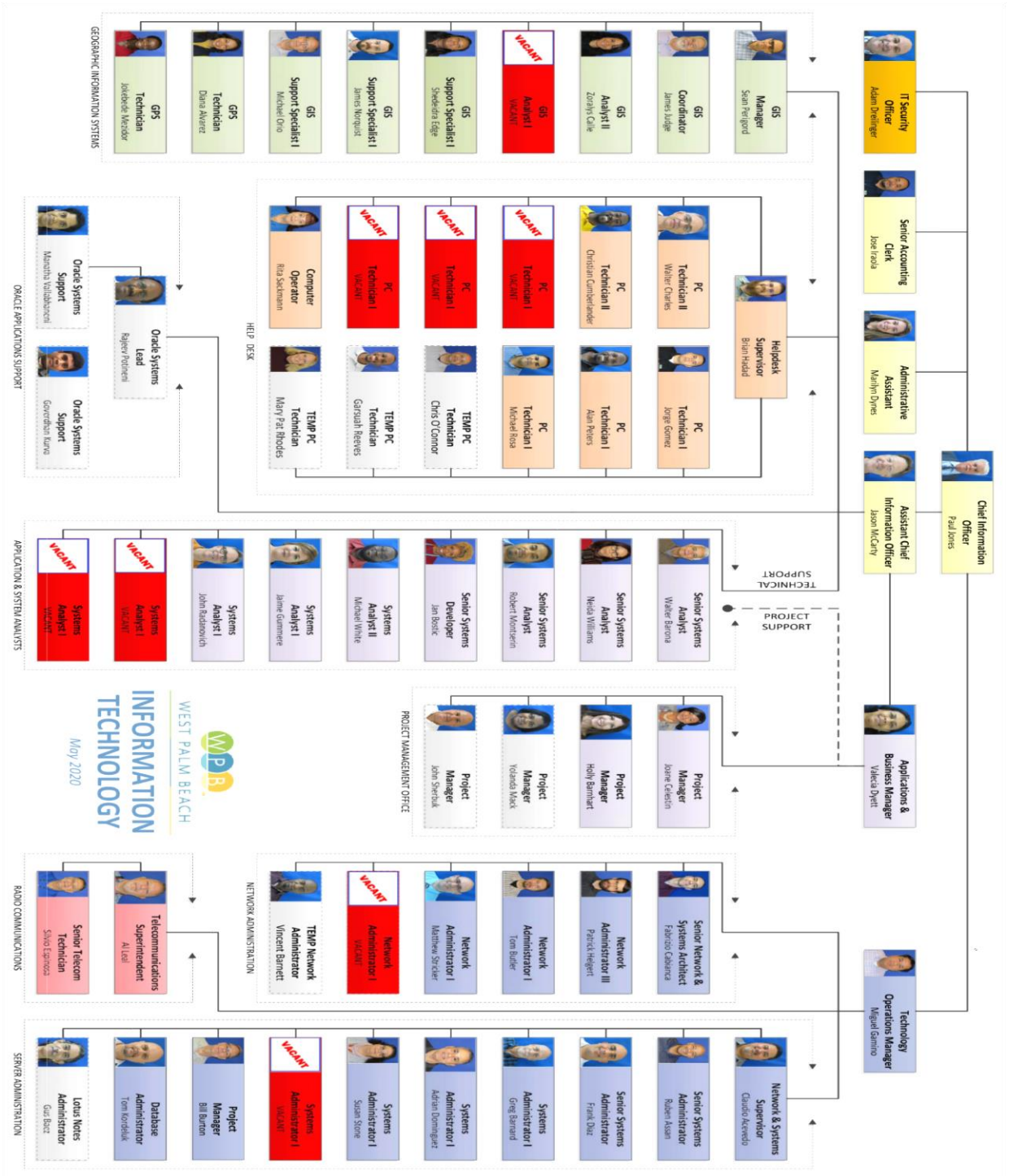
Parking Department Organization Chart



WEST PALM BEACH

Parking Administration

IT Department Organization Chart



Opportunities for Improvement

1. Lack of Required Policies and Procedures

Condition

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 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's standards
- Acceptable Encryption - Data At-Rest Encryption Standards
- Malware/Virus Protection
- Security Monitoring and Auditing
- Passwords

Criteria

Per the Memorandum of Understanding (MOU) and the Florida External IT Security Policy, IT policies are required as related to the following areas to ensure security requirements are in alignment with governing regulations:

- 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

Cause

IT policies and procedures were not established during the audit period (August 14, 2018 to May 31, 2020) under review. We note that IT is currently working on drafting the necessary policies and procedures.

Effect

Policies and procedures set a standard of expectations, ensure compliance with laws and regulations, provide guidance for decision-making, and streamline internal processes. Therefore, not having formal policies and procedures in place creates a culture of disorganization and decreases accountability for the actions of staff members.

Recommendation 1

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.

Management Response 1

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

2. Lack of Third-Party Security Assessments

Condition

Third-Party application service providers typically obtain an independent assessment of their controls and security protocols to ensure compliance with security standards and to identify weaknesses if applicable. This is known as a SOC report that the third-party submits 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, 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 conclude the following areas failed due to not having independent testing to verify security standards prior to or during the use of the IPS software:

- Backups,
- Change Management/Security Patching, and
- Security Monitoring and Auditing.

Criteria

Per the Florida External IT Security Policy, the following should be assessed of the potential third party service provider prior to an agreement of services:

- The Application Service Provider's application infrastructure (hosts, network equipment, etc.) must be located in a physically secure facility and in a locked environment.
- The network hosting the application must be logically or physically separated from any other network or customer that the Application Service Provider may have. This means the authorizing External Entity's application environment must use logically or physically separated hosts and infrastructure.
- The Application Service Provider must provide a methodology and plan for ensuring systems are patched or updated according to industry best practices and guidelines. Patches include, but are not limited to, host Operating System, web server, database, and any other system or application.

- The Application Service Provider must disclose its processes for monitoring the confidentiality, integrity and availability of those hosts.
- The Application Service Provider must provide to the Department information on its password policy for the application infrastructure, including minimum password length, password generation guidelines, and how often passwords are changed.
- The Application Service Provider must provide information on account creation, maintenance, and termination processes, for service, system, and user accounts. This should include information as to how an account is created, how account information is communicated to the user, and how accounts are terminated when no longer needed.
- The Department's application data in the custody of the authorizing External Entity must be stored and transmitted using acceptable encryption technology.
- Connections to the Application Service Provider utilizing the Internet must be protected using any of the following encryption technologies: IPsec, TLS, SSH/SCP, PGP, or any other encryption technologies approved by the Department's ISM.

Cause

The Department was not aware of the security requirements. Further, there were no policies or procedures to ensure that City departments were notified of security requirements particularly when using software that may contain sensitive information.

Effect

When security requirements for the application service provider do not meet the City's standards it may result in business, financial, or legal loss to the organization.

Recommendation 2

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 yearly. In addition, for all future third party service providers used by the Parking Department, Parking management should work with the IT Department to perform a thorough review of the security controls in place to ensure they align with the required standards.

Management Response 2

Agree.

Target Implementation Date: January 31, 2021

3. Improper Termination of Users

Condition

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.
- 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.

Criteria

Per the Florida External IT Security Policy, a user's access shall be promptly disabled and/or removed from systems which access Department information resources, when access is no longer required. Examples include, but are not limited to, termination, transfer, or removal of the duties that require access. Notification of changes in the status of users with established Department credentials is the responsibility of the authorizing External Entity to report such changes to the Department.

Cause

During the audit there were no policies or procedures in place to ensure that staff are aware of IT security requirements or that necessary procedures are in place to protect access to sensitive or confidential data. In addition, it was noted that the termination tickets state access is automatically removed; however, during testing it was noted that access was not removed automatically.

We noted that the Parking Department is currently working with the IPS vendor to remove any unnecessary users with access to the application.

Effect

When a user's access is not promptly disabled and/or removed when access is no longer required it may result in the loss of confidentiality, integrity, and availability of the data.

Recommendation 3

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.

Management Response 3

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 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

4. Lack of Patching Procedures

Condition

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.

Criteria

Per the Florida External IT Security Policy, data should be protected in all forms, on all media, during all phases of its life cycle, from unauthorized or inappropriate access, use, modification, disclosure, or destruction. Security and patch updates help ensure that data is protected.

All development and testing shall be performed on test data and not utilize the Department's production data. Test systems shall be kept physically or logically separate from production systems. However, in some instances there is a need to access the Department's production data in a test environment, which requires an exception from the Department's Chief Information Officer and Information Security Manager. The production environment shall not be adversely affected, and data shall not be altered. Security controls that provide restricted access and auditing shall not be disabled or removed. Confidential or exempt data shall not be used in any test system.

Cause

During interviews with IT management, it was noted that a patching process does not exist. However, it was noted that patching procedures and implementation schedules are currently in process to be put in place.

Effect

Unpatched systems may lead to unforeseen vulnerabilities resulting in unauthorized access to confidential data.

Recommendation 4

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 Response 4

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 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

Auditor's Comment: As a best practice, it is prudent to test patches before introducing them to the production environment.

5. Inadequate Encryption and Secure File Transfer

Condition

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.

Criteria

Per the Florida External IT Security Policy, 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.

Cause

Currently, at-rest encryption is not enabled for the FTP Server. Therefore, when data is stored within the in-scope server, it is not being encrypted appropriately.

It was noted that the IT Department is currently working to implement at-rest encryption to the in-scope server.

Effect

Data that is improperly encrypted or not encrypted at all may result in the loss of confidentiality, integrity, and availability of the data.

Recommendation 5

We recommend that the IT Department enable at-rest encryption for the in-scope server.

Management Response 5

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 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

6. Lack of Separation of Environments

Condition

During the audit period of August 14, 2018 thru May 31, 2020, it was noted that a dedicated Quality Assurance (QA), Development, and/or Test environment did not exist for the City's FTP Server which does not meet the Florida 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.

Criteria

In accordance with FL Admin. Code 60GG-2, all development and testing shall be performed on test data and not utilize the Department's production data. Test systems shall be kept physically or logically separate from production systems. However, in some instances there is a need to access the Department's production data in a test environment, which would require an approved exception from the Department's Chief Information Officer and Information Security Manager. The production environment shall not be adversely affected, and data shall not be altered. Security controls that provide restricted access and auditing shall not be disabled or removed. Confidential or exempt data shall not be used in any test system.

Further, in accordance with FL Admin Code 60GG-2, backups must be periodically tested, at least annually, to ensure that they are recoverable.

Finally, FL Admin Code 60GG-2 states that entities should ensure backups of information are conducted, maintained, and tested.

Cause

A dedicated QA, Development, and/or Test environment does not exist for the City's FTP Server. It was noted that only windows security patches are applied to the in-scope server, which are tested and authorized by Microsoft. However, testing patches is considered industry best practice to ensure that the update does not negatively impact the system.

In addition, there is no current process to test backups for the in-scope server as a dedicated QA, Development, and/or Test environment is not available.

Effect

Untested changes/patches made to the production environment may result in transactions that are not complete, accurate, authorized, auditable or valid. In addition, untested backups may lead to unavailable and unreliable data as the restoration of in-scope systems after a system failure may not be possible due to corrupted backup media.

Recommendation 6

The IT Department should create a test environment for the City's FTP Server to ensure patches and backups are tested appropriately prior to deployment.

Management Response 6

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 Comment: As a best practice, it is prudent to test patches before introducing them to the production environment.

7. Insufficient Password Requirements

Condition

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 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 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 External IT Security Policy requirement of 8 characters.

Criteria

Per the Florida External IT Security Policy, password parameters should align to the following standard:

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

Cause

The password parameters, for both in-scope systems (City's FTP Server and IPS), were not appropriately configured to meet the password parameters established within the Florida External IT Security Policy. Further, we noted that the IPS application is cloud-based, therefore the password parameters for IPS are configured by the vendor (IPS Group). However, the vendor can adjust the password parameters upon request.

Effect

Improperly configured password settings can lead to unauthorized access to resources, programs or data which may result in fraud, theft, misuse of protected information, loss of data or unauthorized transactions. Further, improperly configured passwords can be more susceptible to hacking.

Recommendation 7

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.

Management Response 7

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.

8. Insufficient Knowledge of Users and Permissions

Condition

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 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.

Criteria

Per the Florida External IT Security Policy, all users who access Department data must do so only in conformance with this policy. Only uniquely identified, authenticated, and authorized users are allowed access to the Department data, excluding public access inquiries. Access control mechanisms must be utilized to ensure that users can only access data to which they have been granted explicit access rights.

Cause

The Department was not fully aware of its duty related to IT Security protocol and was thus reliant on the IPS vendor to ensure that appropriate permissions were granted.

Effect

Knowledge of each permission within an application is crucial to understanding if access is appropriate. When management is unaware of the purpose of roles/permissions within an application it may lead to unauthorized access or access that does not follow the least privilege principle (users are granted the least access necessary to complete their job duties).

Recommendation 8

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.

Management Response 8

Agree.

Target Implementation Date: January 31, 2021

9. Insufficient Provisioning Access Requests

Condition

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 request did not meet the access request standards.

Criteria

Per the Florida External IT Security Policy, 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. Established controls must ensure that Department information resources are accessed only by users authorized to do so.

Cause

The departments did not have a procedure in place to consistently ensure that all necessary user information including permissions were included in the request for access.

Effect

A user's access that is not appropriately approved or does not contain critical information such as the user's access, permissions, or rights may result in the user gaining access to information they should not have access to and creates a point of vulnerability.

Recommendation 9

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.

Management Response 9

Agree.

Target Implementation Date: January 31, 2021

10. Lack of User Access Reviews

Condition

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.

Criteria

Per the Florida External IT Security Policy, there must be a documented process for periodically reviewing existing accounts for validity.

Cause

At the time the audit was conducted, neither department had established a periodic review procedure. However, the IT and Parking Departments are currently in the process of implementing review procedures to ensure current access to the in-scope systems is appropriate.

Effect

When a user's access is not appropriately approved it may result in the user gaining access to information they should not have access to otherwise. In addition, when a user's access is not promptly disabled and/or removed when access is no longer required it may result in the loss of confidentiality, integrity, and availability of the data.

Recommendation 10

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.

Management Response 10

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.

Target Implementation Date: January 31, 2021

11. Lack of User Training

Condition

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.

Criteria

The MOU states that:
All persons 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.

All persons 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 data. These acknowledgements must be maintained in a current status.

Cause

The department was not aware of the requirement in the MOU.

Effect

It is important to protect confidential personal data. As such, users should be fully trained and aware of all relevant rules and regulations to ensure consistent application of rules and appropriate use of information. Training is necessary to ensure that users fully understand expectations and associated consequences.

Recommendation 11

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 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.

Management Response 11

Agree.

Target Implementation Date: January 31, 2021