POST AUDIT REPORT
SOFTWARE LICENSES
PAR21-04

December 21, 2020

City of West Palm Beach
Internal Auditor's Office

Beverly Mahaso, Esq. CIA, CFE
Chief Internal Auditor

WEST PALM BEACH

Internal Audit

December 21, 2020

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

RE: POST AUDIT REPORT OF SOFTWARE LICENSES, (PAR21-04)

Dear Audit Committee Members:

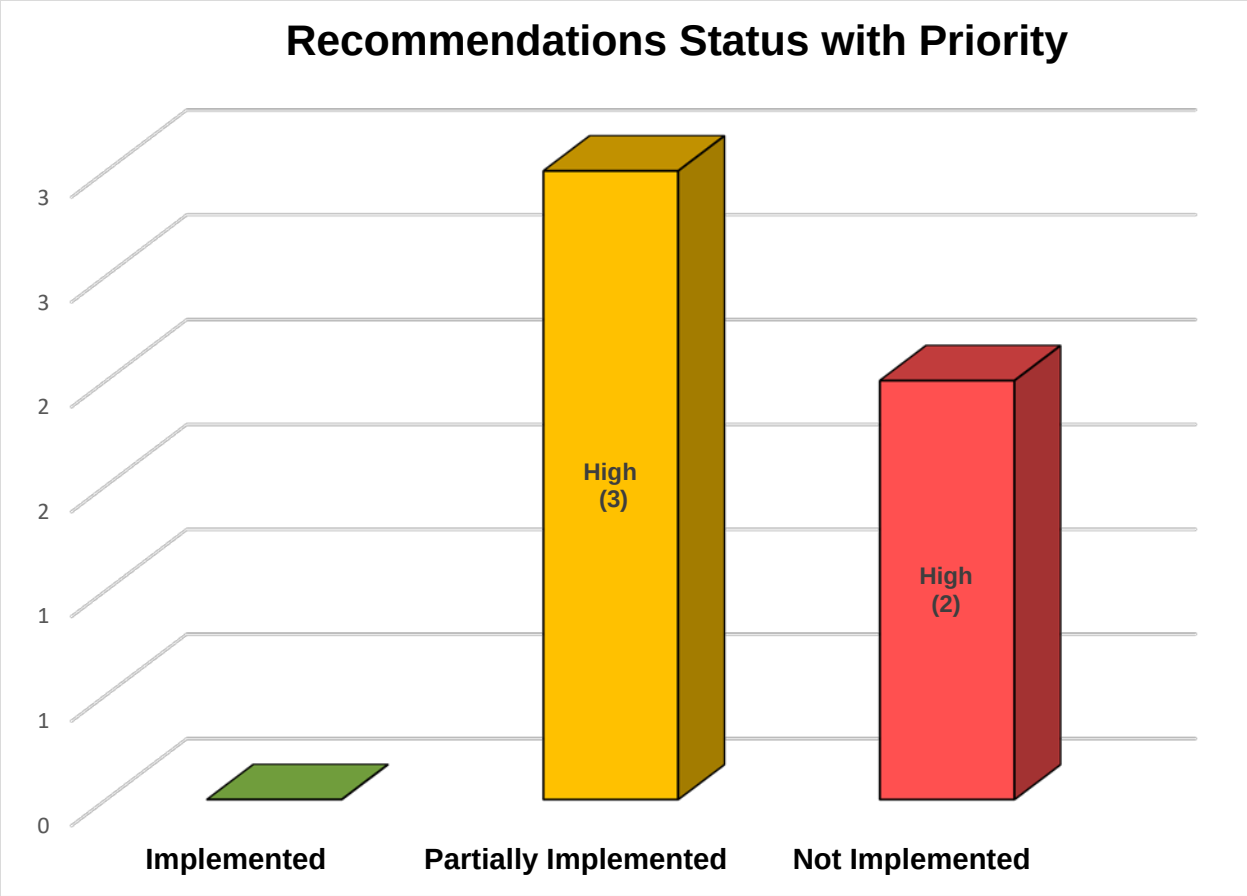
In FY2017, the Internal Auditor's Office released an audit of Software Licenses as managed by the Information Technology (IT) Department (**AUD17-05**). We performed certain procedures, as enumerated below, with respect to activities of the IT Department in order to render a conclusion on the status of the recommendations made as a result of that review.

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

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

The audit contained five (5) recommendations that addressed the audit's findings. Based on the review performed, we concluded that recommendations 1, 2, and 5 were partially implemented and recommendations 3 and 4 were not implemented.

We have enclosed a table listing all the recommendations with the current statuses. We found that management made significant efforts to take corrective action. Further, we note that the IT Department is actively continuing to make improvements. As such, additional steps may have been taken to implement the recommendations after the conclusion of this Post Audit Review. We will conduct another Post Audit Review in approximately 6 to 12 months, resources permitting, at which time we will review all additional changes made after the conclusion of this Post Audit Review.



We thank the personnel at the IT Department for their assistance in conducting this review, and on continuing implementation efforts.

Respectfully Submitted,

s/ Beverly Mahaso
Chief Internal Auditor

cc:

Kelly Shoaf, Commission President
Christina Lambert, Commissioner
Cory Neering, Commissioner
Christy Fox, Commissioner
Joseph Peduzzi, Commissioner

Keith James, Mayor
Faye Johnson, City Administrator
Ricardo Mendez-Saldivia, Asst. City Admin.
Paul Jones, Chief Information Officer

Encl.

Legend
- Implemented
- Partially Implemented
- Not Implemented

POST AUDIT REPORT
SOFTWARE LICENSES
AUDIT RECOMMENDATIONS

No.	Auditor's Initial Condition and Recommendation	Management's Initial Response	Auditor's Status Update
1 High Priority	**Condition:** Our review determined that business applications may have been installed to a greater extent than permitted by license agreements. We performed data analytics to match installed software applications extracted with LanSweeper to the permitted number of licenses in the Software License Key file provided by IT. Deficiencies in the data files included blank department names and/or IP addresses, unmatched application names, errors and/or omissions. Consequently, there were several gaps in the data results when we attempted to match applications. In addition, it appears that both the Software License Key File and the data file of installed software may not have been fully updated due to purchases made without IT guidance. In an effort to better understand the data results, we divided software applications into three groups: Adobe, Microsoft and Other, and found the following: •Of the 1,082 distinct Microsoft applications in the Software License Key file, 949 (88%) were not found in the data file of installed software,	**Management's Initial Response:** We agree with the recommendations. There is already compliance and agreement with Finance and Procurement to route technology related items to IT for approval if the submitter fails to do so. In addition, Local Administrator Rights are now only given to System Administrators within the IT Department, with a few minor exceptions, minimizing the possibility of illegal software being installed. IT is also implementing a software solution that will allow us to have better control on concurrent users for licensed software. This solution also allows for centralized management of software updates and software key updates.	**AUDITOR'S STATUS UPDATE** **PARTIALLY IMPLEMENTED** **UPDATE AS OF 12/2020** Based on the review we completed, we found that this recommendation was partially implemented. IT is improving enforcement of the policy and is currently working on strategically increasing limitations for end users to install software without IT's involvement. We were advised that baseline scans will now be performed. However, additional work is needed to establish a comprehensive policy to include guidance on the approval, purchase, installation, and monitoring of IT software. We were advised that Enterprise agreements with CISCO and Microsoft are being utilized which will help ensure that the City only uses authorized software. We were advised by management that the new target implementation dates will be as follows: -Implementing controls that will permit software installation only by members of the IT Support team: **June 1, 2021** -Scheduling periodic software scans: **April 30, 2021** -Ensuring that software license keys are updated on a periodic basis: **April 30, 2021**

POST AUDIT REPORT
SOFTWARE LICENSES

Legend
- Implemented
- Partially Implemented
- Not Implemented

	•Of the 418 distinct Adobe applications in the Software License Key file, 330 (79%) were not found in the data file of installed software, •Of the 24 distinct Other applications in the Software License Key file, 19 (79%) were not found in the data file of installed software, and •411 out of 104,740 applications identified by LanSweeper did not have a domain identified. As a result of these discrepancies, it may be challenging for IT to manage software and ensure that only licensed software is installed on City devices. We acknowledge IT's on-going efforts to address this long-standing situation by sweeping machines for software and licensing information periodically and on an individual basis. **Recommendation:** Controls over software installation and licensing should be improved by: (1) Working with Administration and Procurement to ensure compliance with the City's Technology Use policy (Section H5) regarding IT pre-approval of software purchases. This should include advance approvals by the requesting Department Director, prior to submittal to IT for approval; (2) Implementing controls that will permit software installation only by members of		-Implementing controls that will ensure the City does not exceed the maximum number of users for each proprietary software product purchased: **April 30, 2021**

POST AUDIT REPORT
SOFTWARE LICENSES

Legend
- Implemented
- Partially Implemented
- Not Implemented

	the IT Support team, particularly when a paid license is required; (3) Scheduling periodic software scans to compare the number of actual installations with valid license agreements; (4) Ensuring that the software license key is updated on a periodic basis to reflect new and/or deactivated license agreements; and (5) Implementing controls that will ensure the City does not exceed the maximum number of users for each proprietary software product purchased. Any exceptions should be determined by IT on a case-by-case basis and supported by a valid business reason.		
2 High Priority	**Condition:** During testing and analysis of software, various non-standard applications were detected on staff computers. Further research indicated that malware and other questionable applications appear to have been installed on some user computers. At least 3 definite malware applications were identified, and 4 other applications did not have discernable business benefits. We brought this to the attention of IT, and the new IT management responded quickly to our concerns. There is a risk that there may be additional questionable applications that were not identified because they were outside the scope of this review.	**Management's Initial Response:** We agree with the above recommendations in principle. Local Administrator Rights are now only given to System Administrators within the IT Department, with a few minor exceptions, minimizing the possibility of illegal software being installed. The IT Department has also recently upgraded its security monitoring application, SPAM filter and will be implementing additional security monitoring tools in the next fiscal year.	**AUDITOR'S STATUS UPDATE PARTIALLY IMPLEMENTED** **UPDATE AS OF 12/2020** Based on the review we completed, we found that this recommendation was partially implemented. Steps taken by IT to address Recommendation 1, will address Recommendation 2 parts 1 and 2. We were advised that there is a system in place to detect malware. However, we found that documentation surrounding malware scanning, detection, and prevention systems has not been completed. We were advised by management that the new target implementation date is **June 1, 2021.**

POST AUDIT REPORT
SOFTWARE LICENSES

Legend
- Implemented
- Partially Implemented
- Not Implemented

	The threat of malware should not be taken lightly. Smaller organizations are at higher risks due to inadequate defensive protection. Over 10 billion malware attacks were detected in 2018. In 2019, a collection of 2.7 billion identity records, consisting of 774 million unique email addresses and 21 million unique passwords, were posted on the web for sale. The average cost of a data breach in the USA will be over $150 million by 2020, with the global annual cost forecasted to be $2.1 trillion. **Recommendation:** The IT Department should: (1) Implement/enforce controls that permit software installation only by members of the IT Support team, (2) Create a policy that requires departments and individuals to purchase and install software only through the IT Support team, (3) Require regular software scans to identify malware and other suspicious applications, and (4) Implement malware detection software throughout the IT environment. Any exceptions should be determined by IT on a case-by-case basis and supported by a valid business reason.		

Legend
- Implemented
- Partially Implemented
- Not Implemented

POST AUDIT REPORT
SOFTWARE LICENSES

3 High Priority	**Condition:** The City utilizes many types of computerized devices in its day to day operations, including workstation PCs, laptops, tablets, and telecommunication devices, to list a few. Many of these devices have a fairly short life cycle due to the ever improving level of technology and are upgraded periodically. Our objective was to link the devices listed in the Servers and Workstations dataset with the corresponding assets in the "Last Seen Data File" provided by IT. Data analytics were used to compare all computer devices in the Servers and Workstations data with the assets in the Last Seen data. We found that at the time of our review, 1,548 devices out of 2,905 devices in the Servers and Workstations data, were not in the Last Seen data (past 7 calendar days). While we acknowledge that some of these machines are likely used by employees who may be on vacation, are not used frequently, are virtual machines, or some other valid business reason, there remains a significant number of machines that are not, but should be accounted for, particularly when considering that the City has about 1,600 to 1,700 employees. If any hardware is set to be retired then that process should occur and IT should have the related software deactivated to ensure that the	**Management's Initial Response:** We agree that the above recommendations are best practice. While providing reports for this audit the focus was on a software inventory, not an inventory of devices. The discrepancies found in the provided information may be attributed to the extensive use of a virtual desktop environment, laptops assigned to field workers, staff on vacation and workstations that may have been retired before an asset management system was implemented to track surplus. The IT Department has implemented a new asset management system that will be tracking software and hardware as they are received and retired.	**AUDITOR'S STATUS UPDATE** **NOT IMPLEMENTED** **UPDATE AS OF 12/2020** Based on the review we completed, we found that this recommendation was not implemented. There is no written policy or process in place. We were advised by management that although IT device purchases, receipts, transfers, returns, and disposals are being tracked, they are missing a dedicated inventory tracking and management process. Once a device is distributed from the IT department, there is no true inventory management and tracking process. Further, there is currently a device location application in place, but there is not a true, dedicated inventory management system. As such, we found that the core components of this recommendation require additional work to better indicate steps towards full implementation. We were advised by management that the new target implementation date is **December 30, 2021.**

POST AUDIT REPORT
SOFTWARE LICENSES

Legend
- Implemented
- Partially Implemented
- Not Implemented

	City is not paying for software that is not used. It should also be noted that laptops, tablets, and phones were not included in this analysis as they may not consistently connect to the City's network. **Recommendation:** The IT department should create and enforce a policy with the associated procedures for the following: (1) device purchases; (2) the receipt of devices in inventory; (3) the transfer of devices to employees; (4) the return of devices from employees to inventory; and (5) the disposal of devices at the end of their useful lives.		
4 High Priority	**Condition:** At present, there are no single-source inventory reports for software and hardware. Different reports provide different items and different counts. **Recommendation:** The IT department should: a) Enforce its policy related to control software maintenance including licensing terms and conditions; b) Create comprehensive, timely, and standard set of reports for both software and hardware, including standard naming conventions. Where possible, these reports should be automatically generated rather than manually generated to reduce errors; and	**Management's Initial Response:** We agree. The IT Department does have an internal policy to control software maintenance and there is a designated staff member that has assumed asset management duties. We agree that reports should be standardized which will be easier to do now that new software and hardware are being entered into our asset management system.	**AUDITOR'S STATUS UPDATE** **NOT IMPLEMENTED** **UPDATE AS OF 12/2020** Based on the review we completed, we found that this recommendation was not implemented. Additional work is needed to address the core elements of the recommendation as indicated in the status of recommendation 3. We were advised that an IT staff member was designated, however, we could not obtain supporting documentation of when the person was designated, or work performed to address the recommendation. IT management did advise that they will actively work on implementing all recommendations, though there are competing priorities. The new

POST AUDIT REPORT
SOFTWARE LICENSES

Legend
- Implemented
- Partially Implemented
- Not Implemented

	c) Designate an IT employee as the inventory management custodian.		target implementation date provided by management is **December 30, 2021.**
5 High Priority	**Condition:** Departments have the ability to purchase and install software on workstations, with access to the City's network, with little or no oversight. **Recommendation:** IT should work with Administration to update the software policy to assign centralized accountability for software purchase and installation to the IT department only, which should be the sole party with administrator rights for software installation. Any exceptions should be made on a case-by-case basis with a valid business reason.	**Management's Initial Response:** There is already compliance and agreement with Finance and Procurement to route technology related items to IT for approval if the submitter fails to do so. Local Administrator Rights are now only given to System Administrators within the IT Department, with a few minor exceptions, minimizing the possibility of illegal/unknown software being installed.	**AUDITOR'S STATUS UPDATE** **PARTIALLY IMPLEMENTED** **UPDATE AS OF 12/2020** Based on the review we completed, we found that IT is improving management and oversight of software installations as described in Recommendation 1. Additional work is needed to ensure consistent enforcement. Updated target implementation dates will be consistent with Recommendation 1.