CITY AUDITOR'S OFFICE

SOFTWARE AUDIT
FIRE AND RESCUE

Report No. CAO 2801-1314-07

May 12, 2014

RADFORD K. SNELDING, CPA, CIA, CFE

CITY AUDITOR

TABLE OF CONTENTS

BACKGROUND 1

OBJECTIVE 2

SCOPE AND METHODOLOGY 2

CONCLUSIONS, FINDINGS AND RECOMMENDATIONS..... 3

1. Non-Business Software Programs – Fire and Rescue 4

2. Unauthorized Business Software Programs - IT 5

3. Unauthorized Shareware or Freeware Software Programs - IT 6

Management Responses 9

Software Audit Fire and Rescue
CAO 2801-1314-07

BACKGROUND

Computer software, or just software, is a collection of computer programs and related data that provides the instructions for telling a computer what to do and how to do it. In other words, software is a set of programs, procedures, algorithms and its documentation concerned with the operation of a data processing system.

Much of the software used has been developed, written, and sold by businesses. This software is often times protected from copyright infringement of software (often referred to as software piracy). These vendors are in the software business and have proprietary rights to their software. Occasionally, this software is taken and used without authorization. Penalties for copyright infringement of this kind vary globally. In the United States, willful copyright infringement carries a maximum penalty of $150,000 per instance. If copyrighted software is on any City of Las Vegas (City) computer, even if the City had no part in the installation, the copyright owner has the right to seek monetary damages against the City.

In order to mitigate penalties of copyright infringement of software the City utilizes Software Asset Management (SAM). SAM is a set of policies, procedures, technologies and people within the organization. SAM allows management to have relative assurance that software products are properly deployed, and unauthorized software is identified and appropriately handled. Without a strong software asset management system there are no assurances as to how many licenses of the software product the entity has and where they are deployed, this can lead to the business using software that is unlicensed. Even though these infringements may be accidental, the owner of the hardware still risks litigation. There is also the issue of the computer user installing unauthorized software on City hardware. The increasing availability of illegal software on-line has made it even more difficult to manage software effectively.

As a part of the enforcement of City policies and procedures, periodic reviews and audits are conducted. These audits could be internal to the Department, by the Information Technologies Department (IT), by members of City Management or by the City Auditor's Office.

The numerous approved policy and procedures governed all aspects of information technology. These policies and procedures were used to audit against.

- IT Policy IT002.2 (issued 11/29/10)
- IT101.1 (issued 3/15/05) govern the City's right to audit all City's owned computers and their contents
- Software control requirements are also stated in Internet Procedure IT122a.3 (issued 3/4/04) referencing various responsibilities
- Internet Policy IT122.2 (issued 3/5/04) reference software downloading

- Policy IT134a.1 Information Security Procedure (issued 2/25/08) requires "Each Department must work with IT to ensure software accountability is maintained by identifying name, version, property code and license number".
- City Policies That Govern Software and Hardware
- Computer Hardware Policy IT108.1 (issued 7/16/10)
- Windows Local Administrator Privilege Policy IT153 (issued 6/25/13)

OBJECTIVE

The objective of our audit was to:

- Identify violations of City software policies and procedures.

SCOPE AND METHODOLOGY

The scope of this audit was limited to a review of current software installed on selected computers assigned or unassigned within the Fire and Rescue. The scope of our work on internal control was limited to the controls within the context of the audit objectives and the scope of the audit.

Our audit methodology included:

- The utilization of SAM software: Microsoft SQL - Server Reporting Services extracts and Audit Wizard Software,
- Research of applicable guidelines, policies, and procedures,
- Interviews of City employees,
- Observations,
- Analysis and detail testing of available data,
- A search of all IT HEAT records (at the time of audit there were 34,156 HEAT records searched). HEAT is a software management database system used in the Information Technology Department to maintain the documentation regarding all computer issues and the documented resolution of those issues. It is the electronic file providing documentation proof of work done.
- No additional databases or methodologies were noted by IT as source for authorized software.

We conducted this compliance audit in accordance with generally accepted government auditing standards except for the requirement for an external peer review every three years. 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.

The exception to full compliance is because the City Auditor's Office has not yet undergone an external peer review. However, this exception has no effect on the audit or the assurances provided.

There are two separate areas of responsibility regarding software installation on city owned computers. Based on current published policy and guidelines IT department has ultimate responsibility over software and monitoring of that software, regardless of the software source. The departments are required to inform and obtain IT approval for desired software.

The report findings are addressed to the department with a request for management responses.

CONCLUSIONS, FINDINGS AND RECOMMENDATIONS

The following conclusions were noted:

Identify violations of City software policies and procedures.

- Thirty personal software programs were found on fifty-five computers. (Finding 1)
- One program lacked proper authorized documentation. (Finding 2)
- Four shareware or freeware programs lacked proper authorized documentation. (Finding 3)

Further information is contained in the following sections.

1. Non-Business Software Programs – Fire and Rescue

Criteria

Computer Hardware Policy (IT108.1)
Policy – "…City of Las Vegas employees may not utilize City computer systems for any purpose other than work related to the City of Las Vegas business unless specifically approved in a separate policy. Personal letter, accounting, checkbook balancing etc., and personal entertainment … are examples of prohibited uses of these devises…"

Computer Software Policy (IT002.2)
Acquisition of Computer Software – "All software acquired by the City of Las Vegas must be purchased through IT."

Conditions

Data Mining on 260 Fire and Rescue computers found the following:

- 30 different unauthorized software programs installed on 55 Fire and Rescue City of Las Vegas computers and details have been given to management.

These software programs did not have a business use and we were unable to determine if they were purchased through IT. The search of the IT HEAT records provided no support showing authorization or installation for the software in Fire and Rescue.

Cause

Failure to follow existing CLV Policy and Procedures

Effect

CLV is at risk by being out of compliance with issued city policies and procedures.

Recommendations

1.1 The identified software programs should be removed from CLV microcomputers by a request being made to IT to remotely remove them.

1.2 Fire and Rescue employees should be instructed on applicable CLV Policies and Procedures related to computer software and hardware use.

2. Unauthorized Business Software Programs - IT

Criteria

Computer Software Policy (IT002.2)
Acquisition of Computer Software – "All software acquired by the City of Las Vegas must be purchased through IT. Software acquisition channels are restricted to ensure that the City has a complete record of all software purchased for City computers so IT can register, support, and upgrade such software accordingly."

Condition

One software programs was found on a computer in Fire and Rescue. It is a medical program which has a business purpose.

- DR Systems Web Ambassador

The search of the IT HEAT records provided no support showing authorization or installation for the above software program.

Fire and Rescue stated they contacted IT for purchase and installation of the software but did not retain any correspondence or licensing documentation.

IT could not provide detail documentation that the questioned software was authorized, purchased, or installed by IT.

Cause

Failure to follow existing CLV Policy and Procedures or inadequate documentation of authorization, purchase, or installation

Effect

CLV is at risk by being out of compliance with software licensing requirements.

Recommendation

2.1 Licenses, authorization, compatibility checking, virus checking, and registry in the software inventory should be completed for the identified program and it

should be in compliance with CLV Policy and Procedure or the software should be removed from CLV micro-computers.

2.2 IT must establish a verifiable system of inventory controls over all types of software programs from software acquisition to installation. Licenses for the identified programs should be obtained and be in compliance with CLV Policy and Procedure or the software should be removed from CLV micro-computers.

AUDITOR'S NOTE: (This is the same recommendation previously made to Information Technologies in the City Clerk Office Software Audit Report. Information Technology staff is currently working on this Procedure. Estimated Date of Completion was revised to March 31, 2014 because IT concluded Fire and Rescue due diligence is far more complex than initially expected.)

3. Unauthorized Shareware or Freeware Software Programs - IT

Criteria

Computer Software Policy (IT002.2)
Shareware/Freeware –
Shareware software is copyrighted software that is distributed freely through bulletin boards and on-line systems. It is the policy of the City of Las Vegas to pay shareware authors the fee they request for the use of their products. Acquisition and registration of shareware products shall be handled the same way as commercial software products.

Freeware software is copyrighted software that can legally be shared and copied without payment to the developer. While the City can legally use such products, they shall only be installed:

With the permission of the Department Director, or designee, and the concurrence of IT; and

After having been checked for compatibility with the City's computing environment by IT; and

After having been checked for absence of viruses by IT.

Installation of freeware shall be registered in the software inventory for the computer. Support and training for such products will not be provided by City Staff.

Condition

Four shareware or freeware software programs were found on computers in Fire and Rescue. These programs may have a business purpose.

- Hand Brake
- Good Search Toolbar
- Google Chrome (2) – IT now allows Google Chrome to be installed, but at the time of the audit Google Chrome was not allowed.

- No evidence exists that the above noted shareware or freeware was authorized by the department director or designee.

- The search of the IT HEAT records provided no support showing authorization or installation for the above software.

- IT could not provide documentation that the questioned software was authorized, purchased, or installed by IT.

- No evidence exists of compatibility checking, virus checking, or registry in the computers software inventory by IT.

Cause

Failure to follow existing CLV Policy and Procedures or inadequate documentation of authorization, purchase, or installation

Effect

- Programs may be on the CLV systems without appropriate authorization.
- Programs could cause compatibility problems with CLV systems.
- Programs may contain viruses because appropriate tests have not been completed.
- Requested licensing fees may not have been paid by the CLV.

Recommendation

3.1 Licenses, authorization, compatibility checking, virus checking, and registry in the software inventory should be completed for the identified programs. They should be in compliance with CLV Policy and Procedure or the software should be removed from CLV micro-computers.

3.2 IT must establish a verifiable system of inventory controls over all types of software programs from software acquisition to installation. Licenses for the identified programs should be obtained and be in compliance with CLV Policy and Procedure or the software should be removed from CLV micro-computers.

AUDITOR'S NOTE: (This is the same recommendation previously made to Information Technologies in the City Clerk Office Software Audit Report. Information Technology staff is currently working on this Procedure. Estimated Date of Completion was revised to March 31, 2014 because IT concluded Fire and Rescue due diligence is far more complex than initially expected.)

Management Responses

1. Non-Business Software Programs – Fire and Rescue

Recommendation

1.1 The identified software programs should be removed from CLV microcomputers.

1.2 Fire and Rescue employees should be instructed on applicable CLV Policies and Procedures related to computer software and hardware use.

Management Action Plan:
The department's personnel who handles IT issues has requested IT to remove the unauthorized software from Las Vegas Fire & Rescue computers. The individual issued requests to IT to remove the unauthorized software. All software was removed by March 20, 2014. In addition, we will instruct Las Vegas Fire & Rescue personnel on applicable CLV Policies and Procedures related to computer software (IT002.2) and hardware (IT108.1)

Estimated Date of Completion: Completed on March 20, 2014

2. Unauthorized Business Software Programs - IT

Recommendation

2.1 Licenses, authorization, compatibility checking, virus checking, and registry in the software inventory should be completed for the identified programs. They should be in compliance with CLV Policy and Procedure or the software should be removed from CLV micro-computers.

2.2 IT must establish a verifiable system of inventory controls over all types of software programs from software acquisition to installation. Licenses for the identified programs should be obtained and be in compliance with CLV Policy and Procedure or the software should be removed from CLV micro-computers.

Management Action Plan:

1) City IT is currently working on procurement for new software that will augment our existing tools for discovery and accounting of licenses. We expect this software to be in place before no later than March 31, 2014, barring any unforeseen circumstances. Once the software is in place we will begin a more effective policing strategy by scanning all existing installations and working to

resolve them (see point 2, below). An additional outcome will be that we will have an accurate electronic inventory of licenses for the myriad software titles we use at the City, and reporting for same.

2) During our initial scans for clean-up, in each case where unauthorized software is discovered, City IT will address by working with the department to either remove or authorize and appropriately license said software. We will authorize software through our electronic service desk, and that will be a permanent record for such authorizations. We will then continue routine scans quarterly. We expect that we can finish all initial scans and mitigation by the end of the calendar year.

3) IT has issued a new policy – IT153 Windows Local Administrator Privilege Policy dated June 25, 2013. This policy will restrict the granting of computer administrator privilege to users. Administrator Rights allows the user to add and delete software to their computers. This will reduce unauthorized software from being added to city computers.

Estimated Date of Completion: By December 31, 2013

AUDITOR'S NOTE: (This is the same response previously made by Information Technologies for the City Clerk Office Software Audit Report. Information Technology staff is currently working on this Procedure. Estimated Date of Completion is by March 31, 2014.)

3. Unauthorized Shareware or Freeware Software Programs - IT

Recommendation

3.1 Licenses, authorization, compatibility checking, virus checking, and registry in the software inventory should be completed for the identified programs. They should be in compliance with CLV Policy and Procedure or the software should be removed from CLV micro-computers.

3.2 IT must establish a verifiable system of inventory controls over all types of software programs from software acquisition to installation. Licenses for the identified programs should be obtained and be in compliance with CLV Policy and Procedure or the software should be removed from CLV micro-computers.

Management Action Plan:

One other factor in the propagation of illicit software is that there is a proliferation of users who have had the administrative ability to install software on their computer without intervention from IT. This practice is largely being discontinued in favor of a more controlled approach and mitigation of some of the problems that were originally solved by allowing administrative control. We are implementing the change with the roll out of new computers and software images, and so we anticipate complete migration to our new policy sometime in the first quarter of 2014.

Also see IT management response to audit finding #2 Unauthorized Business Software Programs

Estimated Date of Completion: By March 31, 2014

AUDITOR'S NOTE: (This is the same response previously made by Information Technologies for the City Clerk Office Software Audit Report. Information Technology staff is currently working on this Procedure. Estimated Date of Completion is by March 31, 2014.)