APPENDIX 1

DISPOSAL OF SURPLUS COMPUTER EQUIPMENT – SECURITY, ENVIRONMENTAL AND FINANCIAL RISK

MAY 4, 2009

TORONTO Auditor General's Office

Jeffrey Griffiths, C.A., C.F.E.
Auditor General
City of Toronto

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Prior information technology audits conducted

The Auditor General's Office over the past number of years has conducted a number of information technology audits including the following:

- Review of Management and Oversight of the Integrated Business Management System (IBMS)
- Disaster Recovery Planning for City Computer Facilities
- The Management of Information Technology Projects – Opportunities for Improvement, Toronto Transit Commission
- Management of City Information Technology Assets – City of Toronto
- Enterprise Case and Occurrence Processing System (eCOPS) Project – Toronto Police Service
- Telecommunication Service Review
- The Migration of the SAP Financial and Human Resources/Payroll System to the City's Agencies, Boards and Commissions
- Toronto Maintenance Management System Application Review
- SAP Financial and Human Resources/Payroll Information System, Post Implementation Review
- Oracle Database Review – Security Controls and Other Issues
- Novell Net/Ware Networks Security Assessment
- Contract Extensions Review – Information Technology
- Windows NT Security Review
- Information Security Framework

Procurement and management audits conducted minimal work on asset disposal

Each one of these audits for the most part has focused on processes related to the procurement of information technology (IT) assets as well as existing information technology systems and controls. Policies and procedures relating to the disposal of information technology is an area which has not received significant audit attention and in view of the potential risks associated with the disposal of IT equipment it was determined that the Auditor General's Office would conduct a high level review of this area.

Three distinct and separate management risks

In general terms, there are three levels of risk in connection with the disposal of IT equipment:

- Security
- Environmental
- Financial

Disposal practices which are illegal in breach of regulations or inadequate could result in legal action, potential financial damages, adverse publicity and loss of public trust.

Security Risk

City information technology assets available for disposal contain significant confidential and sensitive information. Any failure to properly destroy sensitive confidential records and files will have significant consequences to the City on a number of levels not the least of which is privacy legislation.

Environmental Risk

There is little economic value in most technology assets after a relatively short period of time. However, the City is exposed to legal and environmental risks such as hazardous waste, toxicity and corrosivity of IT assets for improperly disposing of technology assets.

Financial Risk

Obsolete IT assets are disposed of through an auctioneer. Unless adequate controls are in place the risk exists that the City may not receive its appropriate percentage of any disposal proceeds.

Further, significant financial penalties may be imposed if confidential information contained on computer hard drives is not deleted and surplus computers are disposed of inappropriately.

City entered into an agreement

In late 2007, the City entered into an agreement with a third party vendor for the disposal of IT assets.

Management of contract requires improvement

During our review of this agreement, we identified a number of issues which need to be addressed. Each one of these issues relate to the management of the contract by City staff.

Process for disposal of assets is adequate

In general terms, the process established in relation to the disposal of IT assets is adequate. However, while the actual process may be adequate, the documentation in support of these processes is deficient and as a result we have not been able to substantiate that the provisions contained in the agreement have been complied with.

Two of the significant provisions in the agreement relate to the deletion and /or destruction of computer hard drives and the disposal of surplus equipment in accordance with environmental legislation. Both of these provisions are extremely important and documentation in support of the actions taken in regard to these provisions require significant improvement.

Conclusion:

There are significant risks involved in relation to the inappropriate disposal of IT assets. In our view, the implementation of the recommendations contained in this report will reduce these risks.

BACKGROUND

Council approved policy for disposal of technology assets

In July 2007, Council approved a report entitled: "Policy for the Disposal of Technology Assets", which recommended that:

1. Surplus working and non-working technology assets be disposed of through a technology asset disposal vendor selected through a competitive process.

2. Staff in the I&T Division continue to make available surplus technology assets as a first priority to City of Toronto grant receiving not-for-profit organizations, second priority to other not-for profit organizations in the City of Toronto, and third priority to our partners (e.g., Soyapongo and Botswana) under the Technical Exchange Program of the Federation of Canadian Municipalities in which the City of Toronto is a participant.

3. The existing policy for the Disposition of Technology Assets adopted by Council in its session of July 22, 23 and 24, 2003, and revised by Council in its session of June 14, 15 and 16, 2005 be superceded with this Information Technology Asset Disposal policy when adopted.

Agreement executed for auctioneering services

In late 2007, the City executed an agreement with a third party vendor "*to provide ongoing auctioneering services for the City of Toronto and its ABCs through public auction and on line auctions on and as when requested basis*".

Schedule C of the agreement with a third party vendor specifically relates to the disposal of IT assets. Schedule C includes specific terms and conditions which "*apply to the Auctioneer's disposal of items or equipment identified by the City as surplus IT assets".*

AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

Our audit methodology included the following:

- Review Best Practices for IT Asset Disposal – The Gartner Group
- Review of Council Reports
- Review of Council approved Policies
- Review of Contract with the third party vendor.

Compliance with generally accepted government auditing standards

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides 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 RESULTS

1. Introduction

Each day, Corporations remove information technology assets from service. Though the reasons are varied (physical failure, planned obsolescence, lease expiration, inability to run new applications or operating systems), the results are the same; a growing pile of surplus electronics.

Risks associated with disposal of IT Assets

Various risks are associated with the disposal of IT assets:

- The risk that information residing on computer equipment such as hard drives is not effectively erased or destroyed.
- The risk that surplus equipment is not disposed of in an environmentally responsible manner.
- The risk of legal liability and significant financial penalties if assets are not disposed of appropriately. In addition the risk exists that the City may not receive its share of the funds received from the disposal of the assets.

2007 Policy approved by Council

In July 2007, Council approved a report entitled: Policy for the Disposal of Technology Assets. This policy was at a high level and initially required that surplus working and non working technology assets were to be disposed of through a technology asset disposal vendor.

The report indicated that *"the I&T Division, through a call process, would like to select a full service disposal firm to remove and dispose of its surplus technology assets with a strong emphasis on hard drive data security and sanitization and environmentally sound disposal procedures"*.

The report also recommended that staff make available surplus technology assets as a first priority to City of Toronto grant receiving not-for- profit organizations, second priority to other not-for-profit organizations in the City of Toronto and third priority to partners under the Technical Exchange Program of the Federation of Canadian Municipalities.

Agreement with a third party vendor

In late 2007, the City executed an agreement with a third party vendor *"to provide ongoing auctioneering services for the City of Toronto and its ABCs through public auction and on line auctions on and as when requested basis"*.

Schedule C of the agreement with the vendor specifically related to the disposal of IT assets. Schedule C included specific terms and conditions which *"apply to the Auctioneer's disposal of items or equipment identified by the City as surplus IT assets"*.

The agreement contains provisions relating to:

- Removal and Storage
- Electronic Wiping
- Refurbish and Resale
- Disposal and Recycling
- Tracking and Reporting.

2. Selection of an Information Technology Disposal Vendor

The recommendations approved by Council requires that "surplus working and non-working technology assets be disposed of through a technology asset disposal vendor selected through a competitive process".

Vendor selected whose main business is the provision of auctioneering services

The vendor ultimately selected through a competitive process was not in fact an information technology asset disposal vendor but rather a vendor whose main business was the provision of auctioneering services. Based on our discussions with management, the I&T Division "piggy backed" on an existing RFP process for auctioneering services and consequently, did not submit a separate proposal for IT asset disposal services. We have been advised however, that the vendor in question was able to provide all of the services the City required even though its main line of business was the provision of auctioneering services. The disposal of IT assets is a relatively specialized business particularly when one takes into account data security and environmental concerns. With privacy laws and data recovery technology in a constant state of development, the selection of a vendor with this type of experience is vital.

Recommendation:

1. **The Chief Information Officer re-evaluate the agreement with the vendor who is currently providing information technology asset disposal services. Such re-evaluation take into account the experience of the vendor particularly in the area of data security and environmental concerns and where appropriate ensure that the vendor is capable of providing the level of service required.**

3. Contract Management Issues

Contract management requires improvement

The Policy for the Disposal of Technology Assets approved by Council consists of a statement that the City will dispose of IT assets through a technology asset disposal vendor and assets will be donated as a priority to specified organizations.

While the above may in fact be a general policy, there is a need to articulate and document a wide range of specific policies and procedures in relation to the actual disposal of IT assets. Further, there is a requirement to ensure that all provisions of the contract with the third party vendor are complied with. The following issues need to be addressed as a priority:

- The agreement provides that the Auctioneer must store all IT equipment in a secure area until such time as hard drives can be wiped/sanitized. Further, the City reserves the right to visit the auctioneer's site at any time during the term of the contract.

Documentation incomplete

Site visits by City staff occurred in May and June 2008. The documentation in support of these site visits for the most part is relatively informal and contains general information in regard to the actions taken by staff.

Staff were unable to provide documentation relating to the site visits which may have occurred subsequent to that time.

Specifically, we identified the following issues in regard to contract compliance.

- The agreement provides that any hard drives that can not be deleted successfully must be destroyed. Further a certificate of destruction must be submitted to the City within two weeks from the date of destruction for each hard drive destroyed.

Documentation deficient

As of the date of our review the City has not received any certificates of destruction. Due to the fact that the vendor is entitled to a commission on the sales of equipment, there is in fact an incentive for him not to destroy equipment. Further the agreement does not state the method of destruction. Documentation of the May 2008 site visit indicates that City staff were not satisfied with the method of destruction and recommended an alternative. There is no evidence that the alternative method was adopted by the Vendor. Unless hard drives are destroyed appropriately it is possible to reconstruct the data on a hard drive.

- A further provision in the agreement requires that the Auctioneer may only sell products containing a hard drive after reporting to the City that the hard drive has been successfully wiped.

We could not locate any written documentation from the Auctioneer that this reporting back to the City had been conducted.

- The agreement requires that monthly reports be completed by the auctioneer showing the status of each hard drive. The agreement provides that reports are to be prepared in a format satisfactory to the City.

Reports have not been submitted by the vendor and in fact the City has not requested such reports.

- Finally, the agreement requires that any “assets , components and material resulting from the assets that are not suitable for re-use must be disposed of in accordance with environmental regulations, and other governing health and safety regulations”

There is no evidence that the City has followed up on this issue with the vendor in order to ensure that there is compliance with environmental requirements.

Recommendation:

2. The Chief Information Officer review all provisions in the agreement with the third party information technology asset disposal vendor and direct the vendor to comply with all provisions in the agreement. Further policies, procedures be established to ensure that the City is able to confirm compliance. Regular audits including the development of audit programmes be conducted to confirm compliance. Documentary evidence of all such compliance audits be retained and approved by supervisory staff.

4. Security Risk

Hard drives must be appropriately deleted or destroyed

Specific instructions for the wiping of data from the hard drives of computer equipment is contained in the contract with the vendor. The instructions require that "the Auctioneer is responsible for wiping the data from the hard drive in a manner that meets RCP TSSIT OPS-11, a DoD Short Standards. At a minimum, a triple pass must be performed". Further, the contract provides that any hard drives that cannot be wiped successfully must be destroyed. Finally a certificate of destruction must be submitted to the City within two weeks from the date of destruction for each hard drive destroyed.

The agreement recognizes that there may be situations where the wiping of data from hard drives may not be possible. Consequently, the risk exists that hard drives which contain sensitive and confidential data are made available for auction. Controls need to be established to ensure that the data on retired hard drives is not available to others.

Various studies conducted in Australia, the UK, Germany and the U.S. have identified the fact that second hand hard drives remain a gold mine for identity thieves. The research suggests that more than a third of all second hand drives are not properly wiped before being resold. The criticism applies to hard drives previously owned by companies as well as individuals. The study found out that 37 per cent of 350 used hard drives bought either online, at retail outlets, or at computer fairs still contained sensitive data. Information retrieved from the drives included bank and credit card information, salary details, medical records, e-commerce, purchase histories and corporate financial data.

Recommendation:

3. The Chief Information Officer, on a random basis, confirm that hard drives submitted to the auctioneer have been successfully erased. Specialized data recovery tools be used to determine whether or not hard drives have been successfully deleted.

5. Environmental Risk

Environmental Legislation must be complied with

Electronic equipment contains a wide range of hazardous material such as plastics, lead, tin, copper silicon, carbon, and mercury. The agreement with the vendor makes reference to the fact that "the City of Toronto is focused on reducing e waste being sent to landfill sites".

The agreement requires that surplus assets not suitable for re-use must be disposed of in accordance with governmental environmental regulations and other governing health and safety regulations such as the "Basel Convention". The Basel Convention is an international treaty designed to reduce the movement of hazardous waste between countries.

While the City recognizes the importance of the environmentally responsible disposal of equipment there is no process in place to ensure that environmental laws are being complied with.

Recommendation:

4. The Chief Information Officer ensure that disposal processes for surplus information technology assets are in conformance with regulatory procedures and all such disposals are supported by an adequate audit trail for subsequent verification by City staff.

6. Financial Risk

The third party vendor is entitled to a commission on the sale of surplus assets. The proceeds after the deduction the vendors of commission is forwarded to the City. The accounting controls relating to the receipt of these funds is inadequate as no reconciliation is conducted of the funds received to the equipment disposed of.

Recommendation:

5. The Chief Information Officer ensure that receipts from the sale of equipment are reconciled to the actual equipment sold.

CONCLUSION

Report contains five recommendations

This report presents the results of a high level review of the processes surrounding the disposal of information technology assets and contains five recommendations.

Addressing these recommendations will further improve the controls pertaining to these assets.