APPENDIX 1

Disposal of Digital Photocopiers – Protection of Sensitive And Confidential Data Needs Strengthening

June 13, 2011

TORONTO Auditor General's Office

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

TABLE OF CONTENTS

BACKGROUND

Hard drives of digital photocopiers contain sensitive and confidential information

Digital photocopiers used in the City contain hard drives similar to a computer hard drive. An image of every document scanned, copied or emailed by the digital photocopier is stored on the hard drive. Therefore confidential or sensitive information either scanned, copied or emailed using these digital photocopiers remains on the hard drive unless steps are taken to remove such data.

2009 review of City practices followed in disposing of surplus IT equipment

In 2009 the Auditor General conducted a review to ensure City practices for disposing of surplus IT equipment aligns with concerns regarding the disclosure of sensitive information and maintaining a safe environment. The report entitled "Review of Disposal of Surplus IT Equipment – Security, Environmental and Financial Risks" contained five recommendations.

The five recommendations addressed the need to:

- re-evaluate the agreement with the vendor providing information technology asset disposal services;
- review all provisions in the agreement and ensure vendor compliance;
- confirm that hard drives submitted to the vendor have been successfully erased;
- ensure disposal processes are in conformance with regulatory procedures and existence of an adequate audit trail for subsequent verification by City staff; and
- ensure that receipts from the sale of equipment are reconciled to the actual equipment sold.

Review focuses on safeguards to protect data stored on digital photocopiers

Digital photocopiers are used extensively throughout the City but are often not considered when concerns over sensitive or confidential information are considered. The Auditor General determined a review focused specifically on controls in place to protect sensitive and confidential information stored on hard drives contained in digital photocopiers would be appropriate.

AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

Extent and scope of our audit

Issues identified in this report are the result of interviews with City staff. The interviews revealed the City's need to implement some fundamental control practices which needed to be addressed.

Compliance with generally accepted government auditing standards

We conducted this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

AUDIT RESULTS

A. Corporate Accountability Needs To Be Clear

Benefits of oversight role in one single division previously reported

Cross divisional issues are usually more effectively managed if the oversight role rests in one single division. The Auditor General has identified the benefits of this control model in a number of other IT related reviews including the Management of City Wireless Technology and Management of City Information Technology Assets.

Responsibility for digital photocopiers not clearly defined

While the Information & Technology Division's responsibility relating to digital photocopiers is not explicitly defined, digital photocopiers are often if not always connected to the City's network and as such the Division is aware when digital photocopiers are acquired. The Information & Technology Division is also responsible for risk management and I&T security.

No single unit has oversight responsibility

Our review however showed that no single divisional unit has responsibility for oversight to ensure information stored on hard drives contained in digital photocopiers is properly protected from unauthorized access or disclosure. Having an appropriate administrative structure supported by clearly defined roles, responsibilities, reporting requirements and coordination would minimize control weaknesses.

Chief Information Officer strategically positioned for assuming oversight role

The City's Chief Information Officer in the organization is strategically positioned to provide the corporate leadership required for the oversight of digital photocopier security.

Recommendation:

1. The Deputy City Manager & Chief Financial Officer assign responsibility for the oversight and protection of information stored on hard drives in digital photocopiers to the Chief Information Officer.

B. A Control Framework Is Required

Digital photocopiers excluded from city-wide control framework for disposal of surplus IT equipment

There is a city-wide control framework for dealing with the disposal of surplus IT equipment which consists of a number of controls including:

- policies and procedures manual
- site visits
- compliance checks
- reconciliations

However, through interviews with City staff we determined that the disposal of digital photocopiers is excluded from this framework.

Control practice at discretion of Division

The process followed for disposing of digital photocopiers and information contained on hard drives is at the discretion of the division. This review did not determine if staff throughout the City are fully aware of the potential risk or whether appropriate steps are always taken to remove sensitive and confidential information. However when discretionary practices are allowed they often lead to inconsistency and variances in processes.

If data stored on hard drives contained in digital photocopiers is not properly removed the opportunity for unauthorized access and disclosure of confidential and sensitive information is increased which may result in:

- a financial liability to the City
- an embarrassment to the City
- a lack of confidence in the City's ability to keep information private and confidential

Recommendation:

2. The Chief Information Officer develop a control framework to ensure the cost effective administration of protecting information stored on digital photocopiers. Such framework should include, but not be limited to the following:

a. a clear definition of the roles and responsibilities of the Information & Technology Division and other City Divisions.

b. expansion of the City's procedures for disposing of surplus information technology equipment to include digital photocopiers

c. procedures for ensuring ongoing verification of removal of data stored on hard drives in digital photocopiers at the time of disposal

CONCLUSION

This report presents the results of our review to prevent unauthorized access or disclosure of data stored on hard drives contained in digital photocopiers.

The two major issues identified in our review include the following:

- lack of centralized oversight for protecting data stored on hard drives contained in digital photocopiers and
- lack of an overall control framework

Addressing the recommendations in this report will provide a cost effective control framework resulting in improved and consistent data protection practices.