

Response to Employee Internet Usage Review

Date:	September 29, 2008
To:	Government Management Committee
From:	Dave Wallace, Chief Information Officer, I&T Division
Wards:	All
Reference Number:	P:/2008/Internal Services/gm08010I&T (AFS #7219)

SUMMARY

This report responds to Council's request to the Chief Information Officer, Information & Technology (I&T) Division on October 22 and 23, 2007 to conduct a feasibility assessment on the monitoring of employee Internet usage, as a result of recommendation 2 in the Auditor General's Report on Internet Usage Review.

Financial Impact

If the City is to implement proactive monitoring and reporting of employee Internet usage, it will have a \$200,000 per annum impact on the I&T Division's operating budget.

The Deputy City Manager and Chief Financial Officer has reviewed this report and agrees with the financial impact information.

DECISION HISTORY

The Auditor General's Office released the Internet Usage Review in July, 2007.
http://www.toronto.ca/audit/2007/internet_usage_review_audit_report_jul2007.pdf

At the October 22 & 23, 2007 Council Meeting, it was moved that the Chief Information Officer of the I&T Division undertake a feasibility assessment to determine the full impact of monitoring employee Internet usage and report back to the Government Management Committee.

ISSUE BACKGROUND

The City's Acceptable Use Policy outlines the professional use of technology, sets out responsibilities, and helps safeguard City assets. The Acceptable Use Policy applies to any employee who is authorized to use the City's information and technology resources and addresses employee Internet use as an I&T resource.

While City employee use of the Internet has always been "logged" (i.e. system logs, back up and recovery procedures), the I&T Division has only retrieved specific Internet usage information from these logs when requested to do so as a result of management concern over an individual's use of the Internet. Such a request for information occurs in the form of a direct request from a Division Director (or higher). This confidential and sensitive activity is coordinated by Human Resources and Legal Divisions, and the data is only retrieved when such action has been approved by both areas. This process is outlined in the Acceptable Use Policy.

Currently, the I&T Division does not proactively monitor employee Internet usage on a systematic basis.

COMMENTS

The I&T Division has investigated the issues associated with the monitoring of employee Internet usage from both the operational implications and the Human Resources, and Legal standpoints.

Feasibility of Proactive Internet Usage Monitoring

The City's current logging and reporting tools in conjunction with the newly implemented User Based Authentication are adequate to accommodate the proactive monitoring as suggested by the Auditor General.

However, the labour effort to undertake the analysis and reporting (i.e. for example - quarterly exception reports), as well as the expected increase in requests for forensic auditing activities as a result of this proactive reporting, will require 2 new full-time employees. It is estimated that this would place an additional \$200,000 per annum pressure on the I&T Division's operating budget.

Implementation of Employee Internet Usage Monitoring

While the City has an Acceptable Use Policy, which provides general Internet usage guidelines, the appropriate technical tools such as User Based Authentication must be implemented and procedures developed which assist management in monitoring employee Internet usage, identifying non-compliance and taking appropriate corrective actions. These procedures have the potential to significantly impact employees and therefore there needs to be a communication and education plan in place for all City Managers and supervisors to ensure consistency of application and response, and adherence to privacy & disclosure regulations.

In addition, any procedures to be developed will need to address the following:

- Selecting appropriate Internet usage criteria or thresholds to generate reports;
- Differentiating between Internet use at the employee's initiative and as assigned by management;
- Differentiating between work-related sites and personal sites;
- Ensuring consistency of application between Divisions, job functions, and individuals;
- Shifting responsibility from an IT focus (i.e. a technical arm's length solution) to a employee's direct supervisor;
- Ensuring posted thresholds do not become permission boundaries; and
- Storing and producing information gathered through this process, including personal information (i.e. complying with MFIPPA legislation).

Status Summary of Councillor Issues

Councillor's issues regarding their responsibilities with respect to the acceptable use of I&T resources have resulted in the following steps being taken:

1. The unblocking of the majority of Internet sites for Councillors, except for sites which distribute or promote spyware, malware or hacking tools.
2. The provision to Councillors of the option of participating in User Based Authentication, which would allow a Councillor's specific profile on Internet access privilege to be used regardless of the log- in location. (i.e. City Hall Office, Constituency Office).

It has been confirmed that the City's Acceptable Use Policy does not apply to Councillors. Meetings with representatives of City Clerk's Office and the I&T Division have taken place to begin the development of an IT Policy for Councillors and Councillors' Staff. This policy will address items such as use of City I&T resources, the provision of IT support services, and other related topics. Such a policy will protect and address their unique needs and requirements regarding the use of City I&T resources.

The City will continue the logging of all computers connected to the City's network as a standard operational procedure. However, as noted previously, this information is not routinely reviewed, except as authorized for specific investigations.

CONTACT

John Davies
Executive Director
Technology Infrastructure Services
I&T Division
Phone: (416) 392-8494
Email: jwdavies@Toronto.ca

John Johnston
Director
IT Strategic Planning and Architecture
I&T Division
Phone: (416) 397-9822
Email: jjohnston@Toronto.ca

SIGNATURE

Dave Wallace, Chief Information Officer