APPENDIX 1

INTERNET USAGE REVIEW

July 31, 2007

TORONTO Auditor General's Office

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The City provides Internet access as a standard feature on all City computers. In 2005, the City issued an Acceptable Use Policy, which provides guidelines on acceptable use of the City's information and technology resources. The policy stipulates that information and technology resources are to be used solely for City business purposes with the exception of limited and occasional personal use.

The Auditor General's 2006 Audit Work Plan included a review of employee's Internet usage, which was assessed as high risk based on reports of inappropriate use to the City's Fraud and Waste Hotline.

The objective of this review was to determine the extent of compliance with the City's Acceptable Use Policy with respect to employee Internet usage pertaining to personal use, visits to inappropriate sites, and excessive use of resources. We analyzed Internet usage logs maintained by the Information and Technology Division, covering four days in 2006, containing over 20 million records for approximately 10,000 users daily.

Our review indicated that controls appear adequate in restricting access to inappropriate sites and activities that use excessive computing resources.

However, current systems and procedures are inadequate to monitor excessive Internet use beyond what would reasonably be considered limited and occasional personal use as allowed in the City's Acceptable Use Policy. Our review indicated that an average of approximately 200 users, two per cent of total users, had over two hours of recorded Internet activity and over 500 page views to over 10 different Web sites that appear to be for personal use per day. In the absence of any standard criteria for Internet use, we considered such usage to be excessive personal use and not in compliance with the Acceptable Use Policy.

There are no proactive measures to investigate individual Internet users suspected of inappropriate use, as the Information and Technology Division investigates user activity only on request. Systems were not designed to identify users, making it difficult to analyze Internet activity where abuse is suspected. Management needs to implement system changes and systematic user monitoring to ensure compliance with the Acceptable Use Policy.

Given the system limitations and the difficulty in further analyzing the activity of the same users identified in this review, we did not investigate any further. In addition, it would be extremely difficult for management to meaningfully investigate the usage identified in our review. We recommend that systematic user monitoring be conducted on a go forward basis.

Information and Technology Division staff has advised that initiatives are already being undertaken that will address certain of the recommendations in this report.

BACKGROUND

The Auditor General’s 2006 Audit Work Plan included a review of employee’s Internet usage. This was considered a high-risk area based on reports of inappropriate use to the City’s Fraud and Waste Hotline.

The City provides Internet access as a standard feature on all City computers. Employees who have access to these computers also have access to the Internet, unless this feature is specifically restricted on that computer.

In May 2005, the City issued an Acceptable Use Policy, which stipulates that information and technology resources, including Internet access, are to be used solely for City business purposes with the exception of limited and occasional personal use.

Limited and occasional personal use is defined as usage that:

- is conducted during non-working hours such as lunch time or breaks;
- does not detract from the user’s work performance;
- does not impair operational efficiency of computer systems;
- does not result in expense to the City; and
- is not an activity that may result in personal gain.

The policy also defines prohibited, unlawful and unacceptable uses of information and technology resources. The policy also provides guidelines on user monitoring. The policy is posted on the City’s Web site and was distributed throughout the City Divisions.

AUDIT OBJECTIVES, SCOPE AND METHODOLOGY

The objectives of this review were to:

- determine whether employee Internet use is in compliance with the City’s Acceptable Use Policy; and

- assess whether adequate controls are in place to ensure adherence to the policy.

Specifically, our review was designed to determine the extent of employee Internet usage that is considered:

- in excess of occasional and personal use as allowed in the Acceptable Use Policy;
- visits or attempts to access inappropriate sites; or
- excessive use of resources, which impairs or interferes with the normal functioning of computer systems.

Our review included an analysis of employee Internet usage for a sample of four days in 2006: April 12, May 12, September 20 and October 19. The review covered Internet usage at City Divisions and excluded Agencies, Boards and Commissions.

Our review focused on Internet activity pertaining to visits to external sites. The review was limited to Internet activity recorded on user logs maintained by the Information and Technology Division, covering approximately 10,000 users. The review did not cover e-mail and intranet activity or visits to the City's own Web sites.

Our audit methodology included the following:

- review of the City's Acceptable Use Policy and related policies and procedures with respect to Internet use;

- interviews with relevant staff of the City's Information and Technology Division;

- review of relevant Council and Standing Committee reports;

- review of similar audit reports in other jurisdictions such as the cities of Ottawa and Edmonton;

- analysis of Internet usage data, using analytical tools such as ACL, Microsoft Access, Excel, and Blue Coat; and

- other procedures deemed appropriate.

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.

AUDIT RESULTS

A. INTERNET USAGE

A.1. An average of approximately 200 users per day appear to have spent excessive time on the Internet for personal use

In the absence of any standard criteria for Internet usage, we set a threshold that users with over two hours of recorded Internet activity and over 500 page views to over 10 different sites that appear to be for personal use, in a day, are considered to be spending excessive time beyond what would reasonably be considered limited or occasional personal use as allowed in the Acceptable Use Policy. Excessive use of the Internet for personal use results in lost productivity.

Our review indicated that approximately 200 computers, or two per cent of all users, had Internet usage that met the criteria we set to be excessive personal use. Due to system limitations, we have been unable to identify all the users or determine whether certain of these computers may be shared. Therefore, the actual number of users that met our criteria may be less than 200. However, our usage data excluded some popular categories such as search engines and reference sites that could have been used for both work and personal purposes. Had we been able to complete a more detailed review of the use of these sites, it is likely that the number of users meeting our criteria would have been more than 200.

A listing of top non-work related categories and top sites in each category for September 20, 2006 is provided in Exhibit 1.

Given the way computers are used and how the related usage information is recorded, it is difficult to be definitive as to the amount of time an individual user spent viewing particular Web sites. As an example, if a user has set up their Internet browser to stay connected to an e-mail or a chat messaging Web site, the log for that computer will likely show that the site is accessed every few minutes and it could appear as if the user is constantly reviewing that Web site. This is related to the software automatically updating the computer for activity on the Web site and happens without the user taking any specific action. In our analysis, we have attempted to make allowance for such activity by setting our thresholds very high and filtering out as much of this automated activity as possible.

In determining the amount of time spent on the Internet for personal use, we used a combination of the following three factors:

Number of hours of recorded activity

We calculated the total minutes of recorded activity on the Internet logs for each user. Each record in the log represents some activity. However, this activity includes graphics and Web advertisements that automatically appear on the screen even without a user necessarily browsing the site. While the number of hours of recorded hits does not necessarily represent actual user activity, it reflects system activity. For our analysis, we used over two hours of recorded activity in a day as a threshold for potential excessive personal use, taking into account the time for lunch and breaks during a normal work day.

Number of page views

A page view represents access to an actual page on a Web site. The number of pages and the number of Web sites visited, combined with the amount of time of recorded hits, provides a better measure of Internet activity. For this purpose, we relied on the Blue Coat analysis tool, which the City recently purchased, to calculate the number of page views allowed. We set a threshold that over 500 page views to over 10 different Web sites in a day would signify an excessive amount of activity. For our analysis, we excluded those categories that are likely to reflect automated activity such as Web advertisements and individual sites with more than 300 page views.

Personal use

In determining whether Internet activity is for personal use, we reviewed a sample of top sites visited and the category assigned to that site by the filtering software used by the City. For the most part, the nature of most of these sites allowed us to reasonably assume that certain sites visited were for personal use. For our analysis, we excluded those categories that are likely work-related such as government, reference or search engines.

It should be noted that each factor taken separately does not necessarily reflect user activity. Therefore, for our analysis of user activity, we considered all three factors combined.

B. MONITORING CONTROLS

B.1. Filtering software appears adequate in blocking access to inappropriate sites

A commercial filtering software, purchased by the City in late 2006, appears adequate in blocking access to inappropriate sites. Previously, the City used free software for this purpose. Our review indicated an increase in the number of sites blocked by the new filtering software, which suggests that the commercial software is more effective in blocking inappropriate sites. As common in the industry, reliance is placed on the vendor for regular updated listings of inappropriate sites.

Certain Internet activities, such as viewing video or listening to audio such as radio stations, require a significant amount of bandwidth and could slow down the City’s computer network. In late 2006, the Information and Technology Division blocked access to video and audio files, resulting in a significant decrease in bandwidth consumption. Access to video or audio files is now granted on an exception basis, upon management approval.

The City also recently followed most organizations in restricting access to Facebook, a social networking forum, which was one of the top sites used by City staff. Our review indicated that other top Internet sites visited pertain to chat or instant messaging and Web mail, which not only use large bandwidth but are also mainly for personal use. We understand that instant messaging carries security risks as hackers could use it to transfer malicious codes that could infect computers with worms and viruses. There is a need for management to review top Internet activities to determine whether further site restrictions are necessary.

B.2. Proactive measures are not in place to identify and investigate individual users for inappropriate use

The Information and Technology Division monitors the overall impact of Internet activity on computer operations and takes corrective action, such as imposing site restrictions, on a system-wide basis. However, there are no proactive measures in place to identify and investigate inappropriate or excessive Internet use at the individual level.

The Information and Technology Division investigates an individual user's Internet activity only upon request. Reliance is placed on Divisional management or complaints to the Fraud and Waste Hotline in identifying users that require investigation. Certain investigations have resulted in criminal charges or disciplinary action.

The City's Acceptable Use Policy provides for user monitoring when there is reasonable belief that computer resources are used inappropriately or in violation of the policy. This reasonable belief could arise from the results of system monitoring. There is a need to implement systematic Internet usage monitoring to ensure compliance with the policy.

B.3. Difficulty in identifying Internet users hinders usage monitoring

Identifying Internet users is an important part of usage monitoring to ensure appropriate corrective action is taken, when necessary. However, identifying the Internet user is difficult or sometimes even impossible.

Internet logs identify users by IP (Internet Protocol) address only, which is dynamic and may change over time. That is, one user always using the same computer may not necessarily always have the same IP address. Information on the user assigned to a specific IP address at a given time is contained in separate logs of users who log on to the network. The difficulty arises when multiple users share a computer, or a portable computer is used in another location, or when a user does not log on to the network as it is possible to access the Internet without logging on to the network. Failure to identify Internet users with inappropriate use hinders the ability to take appropriate corrective action to prevent or minimize recurrence.

The Information and Technology staff indicated that steps are underway to develop a user authentication system that would facilitate the identification of all staff accessing the Internet.

B.4. Improper Internet settings complicate Internet usage analysis

Internet logs provide Internet activity details including dates, times and sites visited. This information is used to analyze Internet usage and assess compliance with the Acceptable Use Policy. While it is important to track visits to external Web sites, there is no apparent operational need to track visits to the City's internal sites.

Our review indicated that Internet logs contain over 20 million records a day, of which approximately 2.8 million or 14 per cent represent visits to the City's internal sites. The recording of this usage information requires unnecessary resources to process and store the information. In addition, this information needs to be excluded from the total activity in order to conduct a meaningful analysis of Internet activity where abuses are suspected. Although the software used to access the Internet can be set to exclude visits to the City's internal sites, it is not being done consistently on all computers.

RECOMMENDATIONS:

1. **The Chief Information Officer implement a user authentication system for all users accessing the Internet.**

2. **The Chief Information Officer, in consultation with the Executive Director of Human Resources Division and the City Solicitor, implement systematic Internet usage monitoring for compliance with the City's Acceptable Use Policy, including:**

   a. **developing criteria for Internet use that may not be in compliance with the policy, particularly relating to Internet time, bandwidth usage and visits or attempts to visit inappropriate sites;**

   b. **utilizing appropriate analysis tools to generate exception reports identifying users with Internet activity deemed to be inappropriate according to established criteria;**

   c. **providing Divisional management with detailed reports and technical support to facilitate review of apparent violations of the City's Acceptable Use Policy;**

   d. **establishing written procedures outlining the types and frequency of management reports on Internet usage and the responsibility for review and follow-up of such reports; and**

   e. **communicating to all City staff reiterating the City's Acceptable Use Policy, clarifying the responsibility of the City and users, and advising of the procedures in place to monitor compliance with the Policy.**

3. **The Chief Information Officer conduct an ongoing review of top sites visited that are likely for personal use, have highly automated activity, or carry**

security risks such as instant messaging or e-mail and determine whether further site restrictions are warranted.

4. The Chief Information Officer take appropriate steps to ensure Internet connections of all City computers are consistently configured so that Internet logs record all Internet activity of all users but exclude visits to City internal sites.

CONCLUSION

Inappropriate use of the Internet exposes the City’s information and technology systems to security risks and could result in liability or embarrassment to the City. Excessive use of the Internet for personal use also results in lost productivity.

The City issued an Acceptable Use Policy, which provides guidelines with respect to Internet use. However, in order to ensure compliance with such policy, adequate procedures must be in place to monitor Internet usage, identify non-compliance and take appropriate corrective action.

Our review identified the need to implement system changes and proactive measures to monitor compliance with the Acceptable Use Policy.

G:\AGO\2007\Reports\Deputy City Mgr & CFO\I & T\Internet Usage Review July 31, 2007 Appendix 1.doc

EXHIBIT 1

Top Non-Work-Related Categories and Top Sites in Each Category for September 20, 2006

Category	Web Site
Chat/Instant Messaging	webmessenger.msn.com ebuddy.com
E-mail	mail.google.com hotmail.msn.com
Business/Economy	tdwaterhouse.ca webmail.uniserve.com
News/Media	www.cnn.com www.thestar.com
Sports/Recreation/Hobbies	www.sports.it espn-ak.starwave.com
Shopping	www.trader.ca toronto.craigslist.org
Arts/Entertainment	www.999mixfm.com www.ezrock.com
Financial Services	www1.royalbank.com wwwec7.manulife.com
Education	webmail.utoronto.ca my.ryerson.ca
Travel	www.aeroplan.com www.expedia.ca

Note: Based on total page views allowed and categories assigned by Blue Coat, for approximately 10,000 users.