



OFFICE OF THE
City Auditor

Employee Internet Usage

February 15, 2007

The Office of the City Auditor conducted
this project in accordance with the
*International Standards for the
Professional Practice of Internal Auditing*

Employee Internet Usage

Executive Summary

Use of the Internet enables employees to access a wide variety of information sources relevant to their official duties. However, along with tremendous advantages, the Internet also provides access to a wide variety of information that is not related to business needs and is harmful or inappropriate for the work place.

The Office of the City Auditor conducted this review to determine whether City of Edmonton employees' use of the Internet is appropriate and in compliance with Administrative Directive A1429B, *Acceptable Use of Communication Technology*.

Based on Internet activity over the 3 month period ended February 28, 2006, the OCA discovered inappropriate and non-work related internet usage by some staff. Inappropriate personal internet use that interferes with employees' work, in addition to being non-productive, can also slow information transfer from the internet, affecting the ability of others to use the internet for business purposes. It also increases the risk associated with Spyware programs and viruses. In some cases, users were found to have accessed inappropriate websites. Accessing inappropriate websites poses an additional risk because the site contents may be offensive to others and could foster a hostile work environment.

This report makes four recommendations to the Corporate Services Department (in cooperation with all departments), to enhance the reporting capabilities of the City's Internet Filtering Software application, to perform additional, periodic monitoring of employee usage, to investigate the activities of employees involved in inappropriate internet usage and to reinforce, through ongoing and periodic communication, the appropriate use of internet access for business purposes and to remind employees that usage is being monitored as part of regular business management practices.

The Corporate Services Department has agreed with the report's findings and recommendations and has developed an appropriate action plan to respond to the concerns raised.

1. Introduction

In its 2006 Annual Work Plan, the Office of the City Auditor (OCA) scheduled a review of Internet Usage. For the period December 1, 2005 to February 28, 2006, the City of Edmonton had approximately 5,400 computer users with work access to the internet. Users include employees who report to the City Manager or City Auditor, contractors and City Council. This access is provided to assist users in performing their stated duties (e.g., email, research). Internet usage is guided by the City's Administrative Directive A1429B, *Acceptable Use of Communication Technology*. The Directive states:

- “The City has NO TOLERANCE for the use of City Assets in a way that could be deemed as offensive or harassing, such as hate mail, racial or ethnic slurs, insults, obscenities, abuse, defamation, threats, sexually explicit materials and internet gambling. Accessing, communicating, creating, distributing, viewing, sending, displaying or downloading of these inappropriate materials will be dealt with severely.”
- “Employees should not expect their communications to be private when using Communication Technology.”
- “The City reserves the right to track, monitor, access, audit, investigate or suspend any Communication Technology use by an Employee.”
- “Use of Communication Technology must be legal, ethical and consistent with the Code of Conduct.”
- “Any violation of this Directive may subject an Employee to the loss of his/her use of Communication Technology and may result in disciplinary action, up to and including termination.”

The City of Edmonton currently uses an industry-accepted internet site filtering software product that is intended to block users from accessing inappropriate web sites. Individual sites are blocked by the software if they match a record within the product's database of inappropriate sites. The database is updated by the vendor on a daily basis. However, it is still possible for users to access inappropriate sites that are not included in the blocked-site database.

There have been a number of recent surveys and studies conducted regarding internet usage in both Canada and the United States. These studies have concluded that internet use in the workplace that is not related to business has risen substantially over the past few years. A Canadian Internet Use Survey¹ conducted in 2005 indicated that just under one-half (49%) of employed Internet users from age 35 to 54 reported accessing the internet from work for personal non-business use. A report² issued by the US Office of the Inspector General in October 2001 regarding internet usage by employees of the US Nuclear Regulatory Commission reported that 52% of internet use was for personal purposes.

¹ Statistics Canada, The Canadian Internet Use Survey (CISU), 2005. (Release date: August 15, 2006.)

² Office of the Inspector General, Use of the Internet at NRC. (Release date: October 15, 2001)

Aside from the obvious risk that a user who spends significant periods of the day engaged in personal internet activity will have a reduced level of productivity and drain IT resources, there are also other, more subtle, risks. Inappropriate internet usage could subject the City to the risk of harassment litigation if other employees are subjected to inappropriate content on their co-workers' computers. This could lead to claims that the City has failed to provide a safe working environment and/or that the conduct of the employees concerned amounts to discrimination against other employees. Such activity could also cause any employees who feel harassed by such behavior to resign and claim unfair "constructive" dismissal.

2. Scope and Methodology

We used data analytics software (ACL) to analyze all of the internet proxy logs and internet filtering software logs for the period December 1, 2005 to February 28, 2006. In all, over 150 million internet log records were analyzed. At the time of this review, the City had a total of 6,677 unique network logon accounts, of these 81% (approximately 5,400) had internet access. As of January 2007, the City had 8,172 unique logon accounts with 82% (6,658) having internet access. Edmonton Police Service employees and Edmonton Public Library employees were excluded from this review.

3. Objectives

Our primary objective was to determine whether City employees were complying with the terms of Administrative Directive A1429B, *Acceptable Use of Communication Technology* when accessing the Internet. Our analysis for this review was designed around two specific objectives.

3.1. Identify non-work related internet usage

Analyse the City's internet proxy logs to identify instances of internet usage that violates the City's Administrative Directive A1429B, *Acceptable Use of Communication Technology*. Our analysis looked for exposure in three areas: productivity loss, bandwidth consumption and data security.

3.2. Identify inappropriate internet usage

Analyse the City's internet filtering software reports and activity logs to identify users with high numbers of unsuccessful attempts to access internet websites that are classified by the filtering software as inappropriate. Examples of inappropriate websites include those that feature sexually explicit, weapons, hate, and criminal activity content as well as 10 other categories³. Our analysis looked for exposure in four risk areas: productivity loss, legal liability, bandwidth consumption and data security.

³ Other categories include: Anonymizers, cults and occult, extreme violence, gambling, hacking, malicious code, personals, dating, spyware, and file sharing.

4. Observations and Analysis

Analysis of employee internet usage is an emerging focus area in corporate governance and control and, as such, most organizations have yet to undertake such a project. Our research did not find any organizations who utilized the same basic methodology or scope as our review. Most other organization internet usage reviews examined total internet activity for only a sample of employees and over a much shorter time frame (e.g., three days).

Our analysis looked at all users over a three-month period but only measured usage on a time spent per-site basis. Our analysis, therefore, is conservative because we did not summarize personal usage at websites where the user spent less than 1000 minutes (16.7 hours) in any given month or those users who spent more than 1000 combined minutes surfing a number of different sites.

Our analysis of the internet logs showed evidence of both inappropriate and non-work-related internet usage abuses. We also found that the reporting capabilities of the City's internet filtering software system were not being fully utilized. Our observations are presented in the following 3 sections. Recommendations resulting from the observations are presented in section 5 of this report along with management's response.

4.1. Excessive Non-Work-Related Internet Usage

We searched the internet logs of approximately 5,400 users to identify those users who were browsing on or obtaining audio/video from a single web site for a monthly minimum of 1000 minutes (16.7 hours) over a three-month period of time. We excluded the standard noon to 1pm lunch hour from the search.

The search of over 150 million logged records indicated that 164 users (approximately 3.0%) were spending a significant amount of time at non-productive sites.

We shared this finding with the Administration and they have developed an action plan to address this issue. Highlights of the action plan are included in the responses to our recommendations. As part of the action plan the Administration has reviewed updated internet usage reports and commenced investigations of identified individual users to determine whether the internet usage is job-related or whether the activity warrants disciplinary action.

The following table shows the top two sites in each of the non-work-related categories accessed by employees during the review period:

Category	Internet Address
Blogging	ads.realtechnetwork.net
Blogging	blogs.msdn.com
Chat	b.mail.google.com
Chat	baym-wm10.webmessenger.msn.com
Investing	kcast.kitco.com
Investing	new.stockwatch.com
Miscellaneous Personal	www.allcomedy.net
Miscellaneous Personal	spui.nscpcdn.com
News	edition.cnn.com
News	www.cbc.ca
Shopping	include.ebaystatic.com
Shopping	shop.com.edgesuite.net
Sports	xxolympicwintergames.hitbox.com
Sports	msn.foxsports.com
Streaming Media	radio.msn.com
Streaming Media	spn.newcapinteractive.com
Video Games	Simpatico.zone.msn.com
Video Games	www.popcap.com

4.2. Inappropriate Internet Usage

The City of Edmonton currently utilizes an internet filtering software product that blocks internet access to most sites that fall within defined inappropriate categories (e.g., sexual content, gambling, hate, and violence). All blocked internet access is logged by the software. We analyzed those logs to determine which employees were being blocked the most frequently. From this analysis, we identified five users with the highest number of blocked sites. We then conducted a detailed analysis of their internet activity for the 3 month period ended February 28, 2006 to determine whether or not they were successfully bypassing the City's internet filtering software and accessing inappropriate sites that violate the City's internet usage policy.

This involved analyzing the complete internet log data for each of these five users. A sampling of the internet sites not blocked by the internet filtering software indicated that these five users were successfully bypassing the filtering software and accessing additional inappropriate sites.

4.3. Monitoring and Reporting of Internet Usage

At the time of the audit, the reporting features of the City's Internet Filtering software were not being used to monitor employee internet usage. However, the City is in the process of replacing its entire internet-delivery technical environment (i.e. including Internet Filtering). The reporting features of the City's new Internet Filtering software will be assessed and implemented by the IT Branch.

5. Conclusion and Recommendations

Providing access to the Internet is an effective business tool. Misuse of the Internet, however, can diminish productivity and increase demands on the internet infrastructure. To minimize the misuse of the Internet, management must take actions to increase users' awareness of the impact of misuse, monitor use, and block prohibited sites and activity. Failure to do so leaves the City vulnerable to threats posed by viruses, the download and use of unlicensed software, viewing of inappropriate material and the potential legal liability associated with such activities.

The OCA believes that the proposed management initiatives will adequately address these risks. In addition, because of the amount of personal internet use identified in this review and the occurrence of prohibited activity in some cases, the Administration will be undertaking further promotion and clarification of the October 25, 2005 Administrative Directive A1429B, *Acceptable Use of Communication Technology*.

The OCA would like to thank the Corporate Services Department for their input and support during this review.

5.1. Excessive Non-Work Related Usage

Recommendation 1	Management Response and Action Plan
<p>The OCA recommends that the Administration periodically conduct scans of internet usage patterns to identify individuals with high amounts of work time spent accessing non-work-related websites.</p>	<p>Accepted Administration Comments: The Administration will implement an internet monitoring program that will ensure a scan of internet usage patterns occurs twice a year. The first scan by the administration has already commenced. The scan focuses on examining internet usage patterns of individuals with high amounts of work time spent on accessing non-work related sites and accessing inappropriate sites. The review is being lead by the Corporate Services Department with the support of the Office of the City Auditor and operating departments. The findings of this scan are being reviewed with operating department managers to determine if the usage is work related. If it is believed the usage is non-work related, a full investigation will occur. In the event it is concluded the usage is non-work related or inappropriate the Administration will take the appropriate disciplinary action. A second scan is scheduled for late 2007 Responsible Party: Corporate Services Department</p>
Recommendation 2	Management Response and Action Plan
<p>The OCA recommends that the City Manager periodically advise employees who have internet access of their responsibility to use work time and technology appropriately and that their usage is subject to monitoring.</p>	<p>Accepted Administration Comments: The Administration is implementing “pop-up” messaging that will appear as employees enter the computing environment. The message will remind staff of the City’s Code of Conduct and the Computer Use Policy. Responsible Party: Corporate Services Department</p>

5.2. Inappropriate Internet Usage

Recommendation 3	Management Response and Action Plan
<p>The OCA recommends that the Administration investigate the online activities of the five identified users with the highest number of blocked sites and, if improper usage is confirmed, take disciplinary action as appropriate.</p>	<p>Accepted Administration Comments:</p> <p>Of the five users identified, three are no longer working for the City and the two remaining staff are being investigated.</p> <p>Planned Implementation: In progress</p> <p>Responsible Party: Corporate Services Department and Operating Department Management</p>

5.3. Management Monitoring and Reporting

Recommendation 4	Management Response and Action Plan
<p>The OCA recommends that the Administration monitor internet usage patterns to identify inappropriate internet activity, and take disciplinary action as appropriate.</p>	<p>Accepted Administration Comments:</p> <p>See action plan for Recommendation 1</p> <p>Responsible Party: Corporate Services Department</p>