PUBLIC SERVICE LABOUR RELATIONS BOARD

AUDIT REPORT OF THE INTERNAL MANAGEMENT OF PERSONAL INFORMATION

MARCH 22nd, 2006

Submitted by:
Samson & Associates
85, rue Victoria
Gatineau, Quebec, J8X 2A3
(819) 772-0044
(819) 595-9094 (fax)
www.samson.ca
samson@samson.ca

TABLE OF CONTENTS

EXECUTIVE SUMMARY

An internal audit of the management of personal information at the Public Service Labour Relations Board (the Board) was carried out during the months of January and February 2006.

The Board is a small organization with a staff of 93. Its personal information holdings are minimal and limited to employee's records, grievance adjudication and complaint case files, appointment of arbitrators and adjudicators, and its Library clients. Personal information is generally defined as *information that is recorded and can be related to an individual.*

The Board is to be applauded for the several initiatives it has taken in keeping with the principles of modern management. In the area of information management, a new structure, direction and a renewed vision for the function has recently been introduced. A Manager of Information Services has been appointed with a mandate to develop strategies, leadership, framework and advice on information management.

There is a need for greater awareness of the responsibility and accountability for privacy of information at the Board. There are few internal policies relating to information management and, more specifically, to management of personal information. Little training and few information sessions are offered to staff on managing information. Employees need to understand their responsibilities relating to the information they create; the various security designations assigned to documents; and, the legislation, policies and procedures that affect the use and protection of personal information.

The role of the Privacy and Access to Information Coordinator needs to be enhanced and the responsibilities transferred to the Manager of Information Services from the current Coordinator, the Chief of Records and Mail. The Coordinator needs to develop policies, provide advice and promote an awareness of the Privacy and Access to Information Acts.

The Board is currently heavily dependent upon paper files. Some concerns were raised about the accuracy with which correspondence is filed by the Records Management Unit. A restructuring of the Unit is underway in an effort to better retain staff and stabilize the operation. The retention and disposal of information by the Board is in keeping with the schedule approved by National Archives. The Board's personal information holdings are accurately described in the Treasury Board's Info Source publication.

Security and access to information is generally well controlled in the Records Management Unit but after-hour monitoring should be introduced to ensure classified information is properly secured in all areas of the Board.

OVERALL OPINION

Based on the audit work performed, it is our opinion that, access to personal information is reasonably well-controlled, personal information is disclosed in compliance with the Privacy and Access to Information Acts, and individuals have access to their own personal information. The Board adheres to a principle of "openness" as all hearings and decisions are made public but, at the same time, keeping in mind the need for privacy of certain personal information.

Improved communications and training on the subject of personal information would foster a greater understanding of employee's responsibilities and the policies that affect the management of personal information.

In our professional judgment, appropriate audit procedures have been followed and sufficient evidence has been gathered to support the conclusions contained in this report. The conclusions are based on the situation that existed at the time of the audit against the audit criteria. The conclusions apply only to the management of personal information activities examined.

This internal audit was conducted in accordance with the Treasury Board Policy on Internal Audit and the Institute of Internal Auditors Standards for the Professional Practice of Internal Auditing.

I. INTRODUCTION

The Board initiated an internal audit of its management of personal information following discussions with the Office of the Privacy Commissioner on whether a Privacy Impact Assessment (PIA) was required. According to the Office of the Privacy Commissioner, the Board did not fully meet the criteria for requiring a PIA in that, despite its expanded mandate, no significant program changes will take place and no incremental sensitive or personal information was being collected. The Board is seeking assurances that the management of the personal information collected and maintained in its delivery of its mandate is in compliance with the Privacy Act and the Access to Information Act, and that the use, disclosure, retention and disposal of personal information meets Treasury Board Secretariat (TBS) policies.

The Public Service Labour Relations Board (the Board) is an organization in transition. April 1, 2005 marked a new era for labour relations in the federal Public service when the new Public Service Labour Relations Act became a reality. The Board is an independent, quasi-judicial statutory tribunal responsible for administering the collective bargaining and grievance adjudication systems in the federal public and parliamentary services. The Board also provides mediation and conflict resolution services to help parties resolve differences without resorting to a formal hearing. As part of its new mandate that came into effect with the introduction of the new Act, a compensation analysis and research function is being established.

In the delivery of its statutory mandate, the Board collects and maintains personal information on individuals who file adjudication grievances and complaints. The information is input into an electronic case management system from forms completed by individuals. Case files (hard copies) are also maintained.

The Board also collects personal information from its employees for the purpose of pay, benefits, staffing, classification, labour relations and performance reviews. This information is maintained in a paper format and some of it electronically using an HR information system.

The new mandate will see the Board begin collecting, compiling, analyzing and disseminating information on rates of pay, employee earnings, conditions of employment, benefits and related data prevailing in the public and private sectors. This information, which is the responsibility of the newly formed Compensation Analysis and Research Services (CARS) Unit, will be maintained electronically.

II. AUDIT PARTICULARS

1. Purpose and Objectives of Audit

The purpose of the audit is to:

- define and document the nature of personal information being collected from clients and employees;
- assess how this information is being captured and protected within the Board's systems; and,
- assess how requests for access to information are handled when personal information is involved.

The objectives of the audit are to determine if:

- the handling of personal information is incorporated in the management framework;
- the retention, protection and disposal of personal information meets security requirements;
- personal information is accessed only by authorized individuals and used for the purpose for which it was collected;
- personal information is disclosed in compliance with the Privacy Act, the Access to Information Act, other applicable legislation, regulations, policies and agreement;
- information on the nature and use of personal information is available; and,
- individuals have access to their own personal information and processes are in place to handle complaints.

2. Scope of the Audit

The audit scope of the internal management of personal information collected and maintained by the Board included registry operations, dispute resolution services, information management, human resources and information technology services**.** Since the Board had yet to conduct any compensation survey activity, at its request, the compensation analysis and research function was excluded from the scope of the audit.

The audit was conducted between January 15th and February 28th, 2006.

3. Methodology and Approach

The following approach was used in carrying out the audit:

1. Reviewed Treasury Board and the Board's policies respecting the management and security of personal information, the Privacy Act, the Access to Information Act and the Government Security Policy.
2. Reviewed the Board's Results-Based Management and Accountability Framework (RMAF), the Report on Modern Management Initiatives in Relation to Expectations of the RMAF, the Threat and Risk Assessment (TRA) of the IT Network, the Physical Security Policy and the IM/IT Plan.
3. Reviewed the Board's Web-site, the Intranet site and its 2005-06 Report on Plans and Priorities.
4. Reviewed the past year's Board's reports on the requests under the Access to Information and Privacy Acts.
5. Reviewed previous internal audit reports conducted at the Board.
6. Reviewed the mapping of processes related to the newly planned Case Management System.
7. Reviewed the Board's Information Management Procedures Manual.
8. Examined selected case files to gain an understanding of their content.
9. Conducted interviews with Board management and staff.
10. Established audit criteria and an audit program to undertake the audit.

III. AUDIT FINDINGS

1. Management Framework

The Board, as a relatively small organization, must rely on a few key personnel each to be responsible for a wide range of duties. The amount of personal information collected by the Board is minimal. Given the Board's limited resource base, it is not realistic to expect the Board to have in place the same magnitude of policies, procedures, controls and focus that would be found in a large government department. Notwithstanding, many of the elements dealing with the process of managing personal information apply to the Board, and the Board needs to be cognizant of the inherent risk it may be exposed to if certain procedures are not implemented.

The personal information collected by the Board consist of employee's personal records, information contained in the grievance adjudication and complaint case files, information relating to Governor in Council (GIC) appointments and information collected by the Library from clients who seek copies of decisions. The Board does not share or collect personal information from other organizations. The Board's personal information holdings are accurately described in Treasury Board's Info Source publication.

The Board is required to keep accurate records to meet its statutory requirements and, when appropriate, to meet public demands concerning accountability for decisions on actions taken. It is also important that sensitive government information is properly protected and access to it controlled. Sensitive information includes certain information about employees or clients. Also with electronic systems and the concern the public has about personal information, risks inherent in these activities need to be identified, assessed and resolved to ensure privacy is respected.

The Board is committed to establishing a modern management agenda and framework that will support its new legislative mandate and provide a shared vision and understanding of expected results. In 2005, the Board developed a Results-Based Management and Accountability Framework and, as well, it prepared a Report on Modern Management Initiatives in Relation to the Expectations of the Management Accountability Framework. This Report examined progress made by the Board with its modern management agenda, developed an inventory of existing practices, policies, frameworks and systems, and identified areas where improvement is required. In relation to information management, the Report indicated a need for a Policy that would clarify the types of documents that needed to be filed, the level of security that should be attributed to the various documents, and the retention or destruction practices that needed to be applied.

The Board has recently created a new position: Manager, Information Management Services. The new mandate sees the position now having overall responsibility for information management services, systems, procedures, training, orientation and advice

to management regarding all organizational records, documentation and material of the Board. This position is expected to develop strategies, leadership, framework and advice on information management. As a first step, it is important that an information management plan is developed that identifies, in measurable terms, expected results, required resources, key activities and time frames to clarify expectations and accountabilities.

The Board has minimal internal policies relating to the management of information and, almost none that relate specifically to managing personal information. On its Intranet site, the Board has a Policy on electronic mail (Email), procedures for responding to enquiries from the public that are not yet case files and procedures for dealing with computer viruses and computer loans. There is also a Policy on the use of Electronic Networks.

The Board's Policy on electronic mail does emphasize that email may be subject to the Access to Information Act and/or the Privacy Act and that, while email is a business communication tool, personal use is permissible but should be kept to a reasonable level. There should be no assumption of "privacy" since the messages are processed and stored in the same manner as business messages. Email transmissions relating to Board business are corporate records and are to be retained in the official corporate filing system "Records Manager", the Board's automated Records Management system. It is estimated, however, that less than 10 percent of these emails are forwarded to the Records Manager. The Board needs to remind staff of the requirement to more fully utilize this mechanism to record information that may be critical to the Board's operations.

The ongoing changes in technology and information overload have brought about an increase in the interest in individual privacy rights. Many commercial enterprises in Canada now have privacy codes or policies that are available upon request to assist in understanding one's rights. It is, therefore, important that the Board inform its employees of their rights in respect to the personal information it collects and uses as spelled out in the Privacy Act.

Employees should also be aware of the steps they can take to protect their privacy and be referred to where they can access additional information such as: how to best manage their P:\Drive; the definitions of classified and designated information; and, the steps needed to protect personal information to avoid Internet fraud. Much information on these subjects is currently available in numerous Treasury Board policies. The Board needs to distill this information and convey to staff through bulletins via its Intranet, topics that would assist individuals in better knowing their rights, the steps the Board takes to protect personal information and steps employees can take to protect their own personal information.

RECOMMENDATION FOR THE BOARD

- **Develop an information management plan that includes, in measurable terms, expected results, key activities, required resources and the expected time frame.**

Management Response #1: The Board acknowledges the need for the establishment of a more formal framework for information management, As noted in this report, the position of Manager, Information Management Services was recently created to provide leadership in this area. The development of an information management action plan is scheduled by March 31, 2007. However, capacity remains an important issue at the Board, as in any other small organization, due to competing priorities. We are hopeful that central agencies will continue to increase the level of guidance and support provided to departments and agencies in the area of information management, hence facilitating the implementation of the action plan in future years.

- **Disseminate information to staff to better inform them of their rights under the Privacy Act and to pass on good ideas, good practices and advice on how to protect personal information.**

Management Response #2: The development and implementation of an awareness strategy on the responsibilities and rights of employees in regards to personal information will be part of the IM action plan. This strategy will include initiatives such as training and the dissemination of information via the Board's intranet site. Proposed Implementation Date: September 2007.

- **Encourage staff through reminders and training that it is important that emails relating to Board business are corporate records and are to be stored in the Board's official corporate filing system "Records Manager".**

Management Response #3: The Board already has in place a Policy on Electronic Mail which clearly defines the Board's expectations in regards to the creation, retention and disposal of emails. This policy is posted on the Board's intranet site. The Board has been using for a number of years an electronic records management system which enables employees to save electronic records in a centralized system. Each time an employee sends an email or saves an electronic document, a message is automatically generated on the employee's screen asking if he or she wishes to save the document as a corporate record, Periodic reminders are sent to employees on the importance of managing electronic records. For example, the Chairperson wrote to all employees in December 2005 to remind everyone of their responsibility to properly document, store and manage all actions and decisions, including decisions made via emails. Furthermore, as part of the orientation session, new employees are informed of the Board's practices and expectations in regards to the management of electronic documents. Notwithstanding the above, the Board acknowledges the benefits of regular reminders on the proper management of

records. The Director, Corporate Service will issue on a quarterly basis a standard message reminding employees of their responsibilities relating to the management of electronic records. Effective Date: June 1st, 2006.

2. Information and Training

There is little training and few information sessions offered to staff on information management. Employees need to know that they are responsible and accountable for the information they create and use to conduct business. This includes electronic information which must be retrieved quickly, consistently and reliably. Proper information management helps everyone to do his/her job better. Each Board employee and their successor rely on having access to the information they need to make informed decisions and ensure efficient delivery of programs and services. A review of past training offered to Board employees on information management shows few employees have attended courses on this subject. An orientation course is given to new employees when they join the Board but the course content on the subject of information management focuses largely on the role of the Records Management Unit. Employee knowledge and comprehension of topics referred to above (i.e. privacy rights, P;\Drive and definitions of classified and designated information) and general information on the Privacy and Access to Information Acts and their application would benefit employees in carrying out their assigned duties.

At the Board, the originator of a document is responsible for determining its security classification. There is no training offered, however, to employees that would allow them to make decisions as to a document's classification. When information is not in the national interest but is exempted or excluded from release under the provisions of the Access to Information or the Privacy Act, the designation could be either "low" sensitive, "particularly sensitive" or "extremely sensitive" information in which case it would be designated Protected "A", "B" or "C" respectively. Classified information, on the other hand, is defined as information that may qualify for exemption or exclusion under both Acts and the compromise of which would reasonably be expected to cause injury to the national interest. In this case, information must be classified as Top Secret, Secret or Confidential and Protected at a level appropriate to the extent of injury that could result if it were compromised.

RECOMMENDATION FOR THE BOARD

- **Provide training to ensure employees understand their responsibilities for the information they create, to ensure that documents are appropriately classified and that those employees having access to personal information, understand the legislation, policies and procedures for the use and protection of personal information.**

Management Response #4: The Board supports the concept of an IM training program and will include it in its IM action plan. Due to capacity issues, the Board

is however limited in what it can develop and deliver when it comes to functional training. A partnership agreement between the Treasury Board Secretariat and the Canada School of the Public Service under the Policy on the Management of Government Information (MGI) implementation initiative has resulted in the development and delivery of some IM training modules focused on functional experts. The Board is hopeful that such partnerships will continue in future years and produce training modules that are directed to employees who perform general information management duties as part of their day-to-day responsibilities.

3. Privacy/ATI Coordinator

The current Privacy/ATI Coordinator is the Chief of Records and Mail Service. The incumbent of this position, who reports to the Manager, Information Management Services, joined the Board in August 2005. Neither the current Coordinator nor the newly appointed Manager, Information Management Services have received training on the role and responsibilities of a Coordinator. Currently, the role of the Coordinator is essentially responding to Privacy and Access to Information requests. There are no documented procedures to follow in the event of a request; however, there are few requests and the Coordinator does make it a point to consult the Board's legal services on all requests.

Dating back to April 1, 2003, the Board has handled 15 Privacy requests and 13 ATI requests, in addition to 28 consultations with other Federal institutions. During this fiscal year, the Board has responded to five Privacy and four ATI requests as well as 10 consultations. Most of this year's requests were received prior to the current Coordinator joining the Board and were handled by a Project Officer who formerly served as the Coordinator and had received the necessary training. Tracking of the requests is managed through an Excel spreadsheet and, in this fiscal year, the Board has only spent a total of 22.5 hours carrying out this activity. All requests are responded to within the 30 day limit and the Board prepares an annual report under the Privacy Act and Access to Information Act which goes to parliament.

In most government departments, the responsibilities of the Privacy and Access to Information Coordinator extend far beyond just responding to requests. Generally, key activities of the Coordinator's Office would include providing advice on access and privacy matters; developing and coordinating policies, guidelines and procedures to manage compliance with both Acts; and, promoting an awareness of both Acts through briefings and guidance. Treasury Board specifies that the Access to Information and Privacy Coordinator should be no more than two reporting levels removed from the Deputy Head, in this case, the Board Chairperson. Currently, the Privacy/ATI Coordinator is further removed in that there is the Executive Director, the Director, Corporate Services and the Manager Information Services between the current Coordinator and the Chairperson.

To ensure that the comprehensive responsibilities of the Coordinator position are more effectively undertaken, the Board needs to consider transferring the role of the

Privacy/ATI Coordinator to the Manager, Information Management Services. Given the compatibility of the role of the Coordinator and Manager positions, it would seem fitting that the Manager, Information Services serve as the Board's Privacy and Access to Information Coordinator. Appropriate training would have to be given to the Manager to ensure optimal effectiveness of this role as Coordinator

RECOMMENDATIONS FOR THE BOARD

- **Appoint the Manager, Information Services as its Privacy and Access to Information Coordinator, provide the appropriate training to the individual to undertake this function and ensure that the current role of the Coordinator position be expanded to develop policies, provide advice and promote an awareness of the Privacy and Access to Information Acts through briefings and guidance.**

Management response #5: The Board sees the roles of coordinator and champion as requiring two distinct set of competencies. It believes that the responsibility of coordinating Privacy and Access to Information requests should remain with the Chief, Records and Mail Services who is responsible and accountable for the management of the Board's records. The Manager, Information Management Services assumes the role of champion for all information management matters, including Privacy and Access to Information, and as such, has the responsibility to develop and put in place the appropriate policy framework. The incumbents of both positions will attend prescribed training by June 30, 2006.

- **Document the processes for handling Privacy and Access to Information requests.**

Management response #6: The documentation of all Board-specific processes remains a priority for the Board. Under the guidance of the Project Officer, the Chief, Records and Mail Services will document each step involved in the processing of Access to Information and Privacy requests by June 30, 2006.

4. Records Management

The Privacy and ATI program delivery process is greatly dependent upon paper files and it is critical that the content of the relevant files is complete. The Records area which retains the case files and is responsible for filing correspondence has been dealing with a relatively high turnover of employees. The organization chart shows that the Records Unit is comprised of six positions, including a Chief of Records and Mail Services, an AS-03, who arrived at the Board in August 2005. The incumbent has an extensive background in records management. Of the remaining five positions, however, three are temporarily filled and one position is vacant

While the Chief of Records and Mail Services indicated that the Unit has been keeping up with the workload, there were concerns expressed elsewhere in the Board about the accuracy with which correspondence is placed in the case files. There was no significant backlog of documents to be filed at the time of the audit. The Board is currently heavily dependent upon paper files and will continue to be so until the new Case Management System is fully implemented next fiscal year. High staff turnover results in a loss of corporate memory and may contribute to documents being misfiled which make the retrieval of information more difficult. Good information management is essential to the efficient and effective delivery of the Board's operations and the Privacy and ATI programs. The roll out of the new Case Management System and the integration of records management and workflow into this new system should boost the Board's ability to find requested information quickly.

A new structure and a new direction for information management within the Board were launched in October 2005. The Manager Information Services position was created and given an expanded mandate. (See above). The Chief of Records and Mail Services now reports to the Manager, Information Services instead of directly to the Director, Corporate Services. A reorganization of the Records Management Unit is also underway that will see one position, the Receptionist position eliminated, and the other job packages rewritten and re-evaluated. It is anticipated these changes will bring about some stability to the workforce in the Records Unit and ultimately result in improved records management.

5. Physical Security and Access Control

Access to the Board's premises is reasonably well controlled. Currently, the Board occupies space on the fourth, sixth and seventh floor of a large office tower. The hearing rooms for adjudication cases and the mediation rooms are on the seventh floor. Perimeter control into the tower in which the Board is located requires individuals to have a building access card. Security guards are also on hand at the entry point to the tower. Access cards are required to enter the Board's facilities on each floor as well as to enter the office areas. Access reports are available to the Security Officer as required. Individual office doors are closed after-hours.

The Director, Corporate Services is the Board's Security Officer and the Manager, Materiel and Accommodation Services is responsible for physical security. A physical inspection of the Board's facilities was last undertaken by the members of the Health and Safety Committee and a report was prepared in December 2005. The report indicated no issues with security. The Manager meets individually with new employees and reviews physical security procedures. He does not undertake an after-hour tour of the premises on a regular basis to observe if classified documents are properly put away. It has been almost two years since this last occurred. Security infractions have not been issued in the past.

Access to the Records Management Unit where files are retained is restricted to the employees working there. Files are released but only to the employees of the Board who have a legitimate need to see the file and the inside cover of files identifies which positions are allowed to access the file. For example, there are between 20 to 25 employees of the Registry Operation and Policy and the Dispute Resolution Services that can access case files. If the person requesting the file does not have the authority to view it, staff from the Records Management Unit are required to fill out an Authorization form and the requester must obtain the signature of an authorized individual. Currently, a charge out card is used to identify who is in possession of a file. A bar coding system is being used to track administrative files. In the new year, the bar coding system will be extended to include case files. There are secure cabinets within the Records Unit that hold, inter alia, files relative to Privacy and ATI requests, administration, executive committee minutes, and appointment of arbitrators and adjudicators.

Most case files in the Records Unit are not assigned a security classification as most hearings and decisions are made public. There are certain cases, however, that are deemed Secret and these are retained in the Chairperson's Office under lock and key.

A list of essential records is also maintained and the records are stored off-site to ensure they are preserved in the event of a disaster such as fire, flood or earthquake. To retrieve these records, the Board must contact the Federal Records Centre of Library and Archives Canada.

Currently, in the Human Resource Services area where employee records are maintained, most files are classified as Protected "A" or "B" and are kept in a secure cabinet with a combination lock and accessed by only a few employees. Sensitive staff relation files are retained by the Manager, Human Resources in a secure cabinet in her office under lock and key. The content of competition files, some of which is personal, is shared with managers to make certain decisions. These files are retained in Human Resources for two years before they are transferred to the Records Unit where they are retained in storage in the basement of the office tower. Keys to this area are appropriately controlled by the Chief of Records and Mail Service. A record of the inventory holdings is maintained on a "Word" data base. If an employee transfers to another government department, the pay file and the career file, is transferred to the new department in a secure envelop "by hand" using a commercial courier. The pay files for employees who are struck off strength are sent to National Archives and the career file is given to the individual.

The Human Resources Section is in the process of documenting its procedures and the automated leave and attendance system is being updated. Currently, employees have "read only access" to their records as does their supervisor and leave forms are submitted to Human Resources for input. Although an interactive system that allows leave requests to be submitted on-line is planned, employees will continue to advise Human Resources of changes to their personal information (e.g. address).

The Manager, Human Resources, expressed concern about the physical security within the Section. The Manager has the only enclosed office in the Section and she is

concerned that the open concept environment does little to ensure privacy when sensitive matters are discussed amongst staff. Contiguous to the Section are the Communications and the Financial Services of the Board. An enclosed meeting room is located near the HR Section.

RECOMMENDATIONS FOR THE BOARD

- **Monitor offices after-hours periodically to ensure all classified information is securely stored.**

Management Response #7: The Board acknowledges the importance of properly storing all classified information and will integrate in its practices a quarterly inspection of offices to be conducted outside regular working hours by the Manager, Materiel Management and Accommodations Services. These inspections will begin in July 2006.

6. Records, Retention and Disposal of Records

The policy on record retention and disposal is set out in the National Archives of Canada Act and the Management of Government Information Policy. Authorization from the National Archives of Canada is required for the destruction of a public record.

The Board has a schedule of all "operational" records which was developed by the Records Unit in cooperation with management and this was approved by National Archives through a submission and the issuance of several Authorities (91/022 and 97/030). When the schedule was approved, the Board operated under its former name, the Public Service Staff Relations Board. The schedule may no longer be valid, hence the Board should verify its validity with National Archives.

The Multi-Institutional Disposition Authorities (MIDA) governs the disposal of "administrative" records. Foremost, the Records Management System used for administration files, contains a retention code indicating the date the file is to be disposed. The schedule is applied to records once yearly or as files are revised pending management's approval. Annually, the Records Unit either will send files to Archives, destroy them or, following discussions with the user, extend the retention period.

IV. SUMMARY OF RECOMMENDATIONS

- **Develop an information management plan that includes, in measurable terms, expected results, key activities, required resources and the expected time frame.**

- **Disseminate information to staff to better inform them of their rights under the Privacy Act and to pass on good ideas, good practices and advice on how to protect personal information.**

- **Encourage staff through reminders and training that it is important that emails relating to Board business are corporate records and are to be stored in the Board's official corporate filing system "Records Manager".**

- **Provide training to ensure employees understand their responsibilities for the information they create, to ensure that documents are appropriately classified and that those employees having access to personal information, understand the legislation, policies and procedures for the use and protection of personal information.**

- **Appoint the Manager, Information Services as its Privacy and Access to Information Coordinator, provide the appropriate training to the individual to undertake this function and ensure that the current role of the Coordinator position be expanded to develop policies, provide advice and promote an awareness of the Privacy and Access to Information Acts through briefings and guidance.**

- **Document the processes for handling Privacy and Access to Information requests.**

- **Monitor offices after-hours periodically to ensure all classified information is securely stored.**