



Nova Scotia Personal Information International Disclosure Protection Act

2007 Annual Report

NS Information Access and Privacy Office

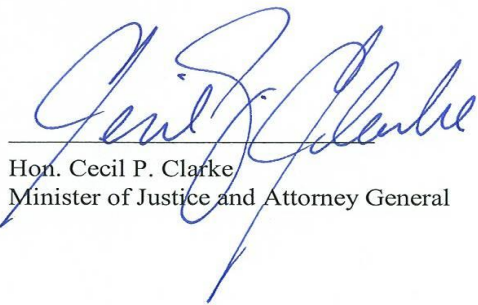
Message from the Minister of Justice

I am pleased to provide the second Annual Report regarding public body decisions to permit foreign access and storage of personal information, as authorized under the *Personal Information International Disclosure Protection Act (PIIDPA)*. *PIIDPA* was passed by Nova Scotia government on July 14, 2006, and became effective on November 15, 2006, for public sector entities and November 15, 2007, for municipalities.

PIIDPA was created to enhance provincial privacy protection activities, and at the same time respond to Nova Scotian concerns about the vulnerability of public sector and municipal personal information holdings to foreign access, storage and disclosure. The Act prohibits public sector entities, municipalities and their service providers from allowing foreign storage, disclosure or access to personal information, except to meet the “necessary requirements” of a public sector or municipal operations.

Under *PIIDPA* subsection 5(3), Nova Scotia public bodies and municipalities are required to report the decision and description of any foreign access and storage of personal information occurring to the Minister of Justice. This report is based on the public body and municipal reports for the calendar year (January 1, 2007 – December 31, 2007) received by the Department of Justice, thus it is our view that the information contained in this report is generally an accurate representation of activity under the legislation.

This report contains a summary of the 33 public sector and municipal entities who reported access or storage of personal information outside Canada, as subject to provisions within *PIIDPA*. This report describes the decisions made, the conditions or restrictions placed, and reasons explained by the public bodies to allow storage or access of personal information in its custody or under its control outside Canada after the *PIIDPA* was introduced.



Hon. Cecil P. Clarke
Minister of Justice and Attorney General

SUMMARY OF SUBMITTED *PIIDPA* REPORTS

- A: Description of the decision of the public body to allow storage or access of personal information in its custody or under its control outside Canada.
- B: Conditions or restrictions that the head of the public body has placed on such storage or access of personal information outside Canada.
- C: Reasons resulting in the head of the public body allowing storage or access of personal information outside Canada to meet the necessary requirements of the public body's operation.

Table 1: Summary of January 1, 2007 – December 31, 2007 Foreign Access and Storage by Government Departments

Department	A (Description)	B (Conditions)	C (Reasons)
Agriculture	The Laboratory Information Management System (LIMS) Project Team (inclusive of Information Technology representation) evaluated software and the selection was an upgrade with the current service provider. This company is housed in the United States and has been our service provider for nine (9) years.	Historically, there was no restriction. The programmer gained access to LIMS via pcAnywhere software. The LIMS system contains clients sample submission and analysis information. The access was only granted for trouble shooting system errors and only at the request of laboratory Services.	Evaluation of proposed systems showed that only three systems met the LIMS criteria. The critical deciding factor to utilize a U.S. firm was the provision of seven unique features, in particular, no data lost and the lowest bid. Laboratory Services deals in surveillance programs for animal health with the Federal Government and is required to maintain a data base of clients and diagnosis. This data would not have been readily transferable into any system other than the windows version of the current system.

Department	A (Description)	B (Conditions)	C (Reasons)
Education (DOE)	<p>The Department utilizes Oklahoma Scoring Services (OSS) software for the purpose of storing and processing information, in support of the General Educational Development (GED) program. The GED is an internationally recognized assessment tool of high school equivalency. The GED credential is accepted by employers across NS and Canada, and serves as an important function for labour mobility. The GED is comprised of five tests that measure the skills corresponding to those of recent high school graduates. There are approximately 1500 tests conducted each year in NS.</p> <p>The department scans the test sheets locally and sends data to OSS over a encrypted Sockets Layer (SSL) connection, or in some cases by traceable courier. The information is stored in a database at OSS located in Norman, Oklahoma for processing and as a record for future reference. Continued storage is required for data retrieval and combining score results for students re-writing tests that were not</p>	<p>The Department has signed a contract with OSS, which stipulates that all information will be kept private and confidential, and will not be released to any third party unless authorized by the Department in writing. The contract also states that only personnel authorized by the department will be provided access to store and retrieve NS information.</p>	<p>The department completed an evaluation of options for the delivery of the NS GED program in November 2001. It was determined that two, suitable for Canadian requirements, GEDTS certified vendors were located in the USA. The application service provider (ASP) model included storage of the data at a vendor location in the USA. At the present time, there is no option of a software solution with data storage in Canada.</p> <p>The other option available in 2001 was to custom develop a system to manage the GED program, and then apply for certification as a testing facility with GEDTS. This option was not chosen due to cost and time constraints to conform to GEDTS program changes in 2002. This would have resulted in an interruption in client service to allow time to design the system and obtain certification from the GEDTS.</p> <p>The department's decision to contract with OSS was based on their extensive experience in GED test scoring,</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>passed successfully. Should the department terminate services with OSS the data will be returned/transferred to the department or another service provider, and removed from the OSS database.</p> <p>The test scoring is completed remotely by OSS and the test results and certificates are transmitted to the department in PDF files for printing locally. The transmission is over a SSL connection or a Virtual Private Network (VPN). The test results and certificates are also available for viewing by authorized DOE staff on the OSS web site, using the same security methods, a user ID and password.</p> <p>In addition, the information is transferred by OSS to the General Educational Development Testing Services (GEDTS) international database, which contains information used for statistical reporting of GED achievements by jurisdiction. This includes gender, age, country, province, number of participants, number passed,</p>		<p>maturity of the software solution, security methods used for transmission of information, and good reputation across educational jurisdictions. In addition, OSS came highly recommended by GEDTS.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>number failed and other information.</p> <p>GEDTS is located in Washington, DC, the international database is housed by Marsys in Miami, Florida, and the backup database is housed by Marsys in San Mateo, California. The international database was established to support the GED program and it is mandatory that jurisdictions agree to send data to GEDTS as part of the GED licensing agreement.</p>		
Finance	Remote access by SAP Support Staff via secure network connections to provide routine SAP support maintenance. With the Province's approval, access occurred several times throughout the reporting period as required to correct or troubleshoot	When SAP Support Staff have reason to access any of the province's SAP systems as part of a problem remediation, all production system transaction access is approved by the Corporate Information Services	Access by SAP Support Staff is required from time to time in order to assist the CIS Division with remediation of technical problems with the SAP systems managed by the Division. This access is controlled by the Province and there is no transaction to SAP systems

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>various problems with the SAP systems. Access was only from SAP's own internal support network and carried out by SAP staff resident in SAP locations, such as the United States, Germany, and India. This remote access very rarely involves access of personal information.</p>	<p>(CIS) Division management and all access activity is recorded in an audit log so that some verification can be done of whether personal information is accessed. In addition, this access occurs over secure network connections that prevent other parties from gaining access to the SAP systems.</p>	<p>permitted without the knowledge and approval of Division management. SAP provides their support services from international locations, in multiple time zones. There is currently no alternative method of support access for the SAP systems that would preclude access from outside Canada. These remote access services are required to meet the mandate of the CIS Division in the performance of services to various public sector organizations who use SAP.</p>
Health	<p>There was no storage of personal information in the custody or control of the Department of Health outside of Canada from January 1, 2007 to December 31, 2007.</p> <p>Between January 1, 2007 and December 31, 2007, seventy-two (72) staff of the Department of Health traveled outside Canada on business and had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise System.</p>	<p>The Department of Health <i>Transmission of Confidential Information by E-mail and Fax Guideline (2004)</i> prohibits the inclusion of personal information contained in e-mail sent outside the GroupWise system unless the e-mail is encrypted and password protected. The Guideline also recommends limiting the inclusion of personal information contained in e-mail within the GroupWise system. Therefore, the amount of personal information held or sent by e-</p>	<p>When staff are traveling for business reasons (e.g., meetings, conferences) they are expected to monitor their e-mail and voice mail where possible in order to fulfill their responsibilities.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
		mail, and therefore available for access while staff was outside the country, should be limited.	
Health Promotion and Protection	<p>There was no storage of personal information in the custody or control of the Department of Health Promotion and Protection outside of Canada from January 1, 2007 to December 31, 2007.</p> <p>Between January 1, 2007 and December 31, 2007, ten staff from the Department of Health Promotion and Protection traveled outside Canada on business and had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise System.</p>	<p>The Department of Health Promotion and Protection <i>Transmission of Confidential Information by E-mail and Fax Guideline (2004)</i> prohibits the inclusion of personal information contained in e-mail, unless the e-mail is encrypted and password protected. The Guideline also recommends limiting the inclusion of personal information contained in e-mail within the GroupWise system. Therefore, the amount of personal information held or sent by e-mail, and therefore available for access while staff was outside the country, should be limited.</p>	<p>When staff are traveling for business reasons (e.g. meetings, conferences) they are expected to monitor their e-mail and voice mail where possible in order to fulfill their responsibilities.</p>
Intergovernmental Affairs	<p>Off site paper document storage contracted with Iron Mountain Canada (subsidiary of the American company).</p>	<p>Iron Mountain is to contact Intergovernmental Affairs upon the receipt of a subpoena or similar order unless such notice is prohibited by law. Confidential information held by Iron</p>	<p>Due to limited storage space for business records, Intergovernmental Affairs required off site storage. At the time of the contract, 2006, there was no Canadian-owned competitor in NS and Iron Mountain is considered to be the</p>

Department	A (Description)	B (Conditions)	C (Reasons)
		<p>Mountain is to be held in confidence as per the agreement. Iron Mountain will use the same degree of care to safeguard this information as it utilizes to safeguard its own confidential information.</p>	<p>industry lead.</p>
Justice	<p>a. Under the <i>Child Abduction Act</i>, c. 67, R.S.N.S., 1989, implementing the Hague Convention on the Civil Aspects of <i>International Child Abduction Act</i>, information in two child abduction files was exchanged during this fiscal year. One involved a situation in which a child was removed to Romania from Canada; the other in which a child was removed to Canada from France.</p>	<p>a. No restrictions or conditions are placed on the information. The information supplied to the foreign Central Authorities and counsel for the parents is for the purpose of commencing a court application. Information was received for the same purpose.</p>	<p>a. A lawyer for DOJ is the Central Authority responsible for discharging the duties imposed by the Convention for Nova Scotia. The duties involve co-operating with the Central Authorities of foreign contracting states in securing the prompt return of children (Art. 6), and include the exchange of the parents' and child's personal and other information with the foreign contracting state, particularly the personal information and documents of the parents and child required (Art. 8) in the application provided to the foreign Central Authority to commence the foreign Court application for the return of the child. Personal information may be exchanged in facilitating access between the left behind parent and the removed child. Additional documentary or other information may be required by</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>b. Correctional Services staff traveled to Newport, Rhode Island with members of the Emergency Management Office November 26 to 30th and may have accessed personal information through e-mail during that time.</p> <p>c. Mammoth Communications was awarded the contract for Electronic Supervision of Offenders and iSECUREtrac, the subcontractor; configured and installed a turnkey host monitoring system in Mammoth's designated monitoring station facility in Halifax, Nova Scotia. All offender data resided on that system and nowhere else. Permission had been granted to</p>	<p>b. Remote access to GroupWise is protected by username/ password authentication, and is delivered over an SSL-encrypted link via the secure Blackberry GroupWise server.</p> <p>c. 1. Mammoth Communications' project manager was the only person authorized to establish user accounts (logins and passwords) for the host monitoring system.</p> <p>c. 2. Only designated Mammoth Communications and Nova Scotia Department of Justice</p>	<p>the foreign Central Authority, counsel in the foreign jurisdiction, or the foreign Court in determining the issues of habitual residence or grave risk of harm if the child is returned. When requested, the Nova Scotian Central Authority attempts to acquire, or facilitate the acquisition of, the requested information and provide it.</p> <p>b. Staff monitor their e-mail and voice mail when they are out of the office to fulfill their work responsibilities.</p> <p>c. This access was necessary to ensure optimal service and to maintain automated monitoring systems that communicated system issues, such as hardware failures, software abnormalities, or other operating environment issues that may arise. ISECUREtrac personnel required access to the operating system and software in order to complete regular</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>designated iSECUREtrac U.S. Customer Service personnel, located in Omaha, Nebraska, to temporarily access the Nova Scotia host monitoring system only for the purpose of trouble-shooting/ customer support and further, such temporary access was in accordance with a signed agreement restricting such access to the host monitoring system.</p>	<p>personnel had ‘permanent’ user access to the host monitoring system. (iSECUREtrac U.S. Customer service personnel did not have permanent login or password information to access the Canadian system.</p> <p>c. 3. Occasionally, designated iSECUREtrac U.S. Customer Service personnel were granted temporary access and only for the purpose of trouble-shooting or customer support:</p> <ul style="list-style-type: none"> i. such temporary access was issued by Mammoth’s project manager only; ii. Project manager must document the purpose of the access, the person to whom the access was granted, and the time, date, and duration of the access; iii. Project manager must immediately notify Nova Scotia Department of Justice of all relevant details of the access; 	<p>system maintenance functions required to ensure mission critical operation of the system.</p> <p>This contract was terminated on December 10, 2007 and the contractors indicated in the report are receiving no further information.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>d. JEMTEC Inc. was awarded the contract for Voice Verification of Offenders. All personal information is stored in secure databases located in secure Monitoring Centres owned/operated by JEMTEC (including its subcontracted monitoring services), BI and Biometric Securities - located in Toronto, Canada, Boulder, Colorado, US and Dublin, Ireland respectively.</p>	<p>iv. Project Manager must verify that access has been terminated after the support function has been completed.</p> <p>d. 1. JEMTECS' project manager and the Provincial Electronic Supervision Coordinator must be the only persons authorized to establish user accounts (logins and passwords) for the host monitoring system .</p> <p>d. 2. JEMTECS' Project Manager must immediately notify DOG of all relevant details of any unauthorized access. JEMTECS' Project Manager shall document the reason the access occurred, the person/agency who accessed the information, and the time, date and specific data compromised and duration of the access. JEMTECS' Project Manager shall verify what steps have been taken to prevent further unauthorized access.</p> <p>d.3. The VoiceID system</p>	<p>d. This access is necessary to ensure optimal service and to maintain automated monitoring systems that communicate system issues, such as hardware failures, software abnormalities, or other operating environment issues that may arise. JEMTEC Inc and its subcontractors require access to the operating system and software in order to complete regular system maintenance functions required to ensure mission critical operation of the system.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>e. The Director of Maintenance Enforcement has an obligation, pursuant to the <i>Maintenance Enforcement Act</i>, to enforce all maintenance or support</p>	<p>contains a native journal function to allow system and program management users access to an audit trail of all changes made to an individual's file or its data contents (e.g., offender address, contact information, scheduling of calls, termination of offenders from the program", as well as who made the change, when it was made and what the change consisted of. This provides senior administrators with a tracking tool for quality control and data security purposes. Access to the systems is via a standard internet browser with 128 bit SSL encryption, with predefined timeouts to lock out users after periods of inactivity after they have logged in, for security purposes.</p> <p>e. If the Payor of support resides outside the Province, the Director may be required to send personal information to the</p>	<p>e. The Director is also required to send personal information to reciprocating jurisdictions in order to comply with the statutory obligations and duties under</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>orders which have been filed for enforcement with the Director. In discharging this statutory obligation and duty, the Director may be required to send personal information to a jurisdiction outside the Province, including outside of Canada. The Director has the authority under the <i>Maintenance Enforcement Act</i> to disclose personal information to a reciprocating jurisdiction for the purpose of enforcing a filed maintenance order.</p> <p>The Director is also required to enforce maintenance or support orders which have been registered for enforcement in Nova Scotia, under the <i>Interjurisdictional Support Orders Act (ISO Act)</i>, by, or on behalf of, support recipients who reside outside the Province, in the reciprocating jurisdiction.</p> <p>The Designated Authority (Court Services), designated by the Minister of Justice pursuant to the NS <i>Interjurisdictional Support Orders Act (ISO Act)</i>, sends personal information</p>	<p>jurisdiction in which the Payor resides, if that jurisdiction has been declared a “reciprocating jurisdiction” under the regulations made pursuant to the <i>ISO Act</i>. The personal information sent is required by the reciprocating jurisdiction in order to enforce the maintenance order in that jurisdiction. A jurisdiction may be declared a “reciprocating jurisdiction”, pursuant to the <i>ISO Act</i>, if the Governor in Council is satisfied that the laws in the reciprocating jurisdiction are substantially similar to those in the Province respecting the reciprocal enforcement of support orders.</p>	<p>the <i>Maintenance Enforcement Act</i>.</p> <p>The Designated Authority is required to send personal information to reciprocating jurisdictions in order to comply with its statutory obligations and duties under the <i>ISO Act</i>.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>to jurisdictions outside the Province, including outside Canada, for the purpose of the enforcement, establishment and variation of support or maintenance orders on behalf of Nova Scotia residents. The Designated Authority can only send personal information to a jurisdiction that has been declared to be a “reciprocating jurisdiction” by regulations made pursuant to the <i>ISO Act</i>.</p> <p>The personal information sent by the Designated Authority outside Canada is the personal information which is contained in the documents that are submitted to the Designated Authority by a person who is seeking to enforce, establish or vary a support or maintenance order, where the other party resides outside Nova Scotia. The documents are submitted to the Designated Authority with the request that same be sent to the reciprocating jurisdiction in which the other party resides. The Designated Authority is required, and authorized, under the <i>ISO Act</i>, to thereupon transmit or send these documents to the reciprocating</p>		

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>jurisdiction, as requested. The body to which the documents are sent in the reciprocating jurisdiction is the government body, or in some cases, the court, in the other jurisdiction, which has been designated by the reciprocating jurisdiction.</p>		
<p>Natural Resources</p>	<p>a. Four staff members traveled outside Canada on business and had ability to access personal information carried on e-mail or stored in GroupWise via remote e-mail system.</p> <p>b. Three staff members traveled outside Canada on pleasure and had ability to access personal information carried on e-mail or stored in GroupWise via remote access to GroupWise e-mail system.</p> <p>c. Off site record storage contracted with Iron Mountain Canada (subsidiary of the American company).</p>	<p>a. Remote access to GroupWise is protected by username/password authentication, and is delivered over an SSL-encrypted link.</p> <p>b. Remote access to GroupWise is protected by username/password authentication, and is delivered over an SSL-encrypted link.</p> <p>c. Iron Mountain must safeguard and maintain protected storage of the Department's records. Iron Mountain Canada Corporation confirms that personal information is maintained and disclosed in accordance with our contractual arrangement in</p>	<p>a. When staff are traveling for business reasons they are expected to monitor their e-mail and voice mail where possible in order to fulfill their responsibilities.</p> <p>b. When staff is traveling for pleasure they are sometimes required to maintain contact with operations.</p> <p>c. Off site storage of backup media/microfilm is required as part of the Disaster Recovery Program. The off site storage is required to ensure recovery of vital records can be recovered should an incident occur.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
		compliance with all applicable privacy legislation.	
Service Nova Scotia and Municipal Relations (SNSMR)	<p>a. The Inter-provincial Record Exchange (IRE) system allows Canadian motor vehicle jurisdictions to securely query other jurisdiction's driver and vehicle records. The Canadian Council of Motor Transport Administrators (CCMTA) disseminates the IRE information, administers the system and operates the secure network. There is a partnership arrangement with the American Association of Motor Vehicle Administrators (AAMVA) to extend the IRE system to the US.</p> <p>b. Digimarc, of Fort Wayne, Indiana, was awarded the contract to provide Photo Licence/Photo ID equipment, software integration and support services for the Registry of Motor Vehicles in 1999. The current contract expires in 2008 and will be replaced with a new contract under the joint</p>	<p>a. CCMTA acts as the clearing house for all queries so that jurisdictions do not have direct read access to another jurisdiction's system. Queries are forwarded to/from member jurisdictions only (CCMTA & AAMVA). Queries are pre-formatted and specific as to what information is displayed. CCMTA has contracts with each of its member jurisdictions that conform to the jurisdictions' privacy legislation concerning disclosure and consent.</p> <p>b. Access from the Fort Wayne location is restricted via VPN username/password to these two support technicians and on the Oracle server by a privileged account username/password. Access will be in response to escalated support calls only.</p>	<p>a. Promotion of road safety and law enforcement so that a driver's license or vehicle permit may not be fraudulently transferred from one jurisdiction to another.</p> <p>b. Access by Digimarc is an operational requirement in response to Photo Licence/ Photo ID outages that affect the delivery of customer service.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>Atlantic Canada Photo License Project. One component of the system, the Photo License Oracle server that stores client photos, digitized signatures, personal information, and Driver Master Number is located at the Provincial Data Centre in Halifax. In 2006, two Digimarc support technicians were provided remote access via VPN to provide tier II/III support. Routine maintenance and support for this system is provided by a local Digimarc field technician, with the Fort Wayne technicians acting as back-up, or managing escalated problems the local technician isn't able to resolve.</p> <p>c. Nine SNSMR staff members travelled outside Canada during the reporting period and accessed GroupWise e-mail from a laptop or Blackberry™ while away.</p> <p>d. An American company, Tyler/CLT, was given controlled access to Assessment for the purpose of converting and transferring that data from the Assessment legacy system to</p>	<p>c. Remote access to GroupWise is protected by Username/Password authentication, and is delivered over an SSL-encrypted link.</p> <p>d. Contractor access is only allowed through a restricted and audited VPN account. Contractors can only access a terminal server, which has been configured for the purposes of</p>	<p>c. To maintain contact with operations.</p> <p>d. The iasWorld system was the only Computer Aided Mass Appraisal (CAMA) system that would meet all the Assessment Divisions requirements. Competing Canadian systems were</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>the new iasWorld system. Tyler/CLT continues to have controlled access to the system, which houses Assessment data for the purpose of servicing and maintaining the system. For security reasons all data remained in Canada, and remote access by Tyler/CLT was tightly controlled.</p>	<p>doing the data conversion. The terminal server is configured to not allow data transfers to other computers, i.e., the contractor cannot mail or copy the file to themselves or another network. Contractor activity is reviewed and monitored via the audit logs.</p>	<p>examined during the RFP process, but did not meet requirements. The American company Tyler/CLT serviced the Assessment legacy system and produced the core CAMA component of the new iasWorld system. Therefore they were the only organization with the expertise to convert the data from the old system to the new, and to service iasWorld on an ongoing basis.</p>
<p>Tourism, Culture and Heritage</p>	<p>a. Decision to allow primary service provider (Unisys Canada Inc.) for Internet resource Nova Scotia Historical Vital Statistics Online (NSHVSO) operated by NS Tourism, Culture and Heritage, (Archives and Records Management Division), to out-source to service sub-provider (Skipjack, Cincinnati, Ohio, USA), part of the transaction processing, and storage during processing, of credit card information collected from service clients during online interactive commercial activity.</p> <p>b. The Department has contracted Cloutier Direct Inc. (CDI) of</p>	<p>a. No access to or storage of credit card information by service sub-provider outside Canada except as required to carry out and verify online credit card transactions with NSHVSO service clients.</p> <p>b. Names and addresses may only be used to fulfill requests</p>	<p>a. Commercial component of NSHVSO service is dependent upon client's ability to prepay for copies online via credit card transaction conducted in real time. Due to the global character of today's financial services industry, it is extremely unlikely that online credit-card transactions can be completed and verified without the personal information collected during transaction processing being stored, accessed from or disclosed outside Canada.</p> <p>b. The Department has contracted CDI to provide fulfillment services to ensure</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>Scarborough, Maine to mail Nova Scotia tourism information to people who have requested Nova Scotia information from the U.S. and internationally. Requests are received through our customer contact system, call centre, which is based in Halifax; through the Novascotia.com website and through regular mail requests. On a daily basis CDI downloads, from our contact centre, US and International requests and sends out the requested information.</p>	<p>received by the Department. The Department owns the database. CDI may only use the names and addresses once approval is received from the Department.</p>	<p>that the potential visitor to Nova Scotia receives their literature promptly in a cost effective way. The Department previously fulfilled US and International requests from Canada and the delivery time was too long and too expensive for the service received.</p>
<p>Transportation and Infrastructure Renewal</p>	<p>a. Telecom Service Group awarded the contract to monthly re-bill government users' telecommunication services to Symphony Services, located in Dallas, Texas. Symphony Services will have access to the current Tru Server application to complete the transition to the Expense Management System (EMS). The server is located in Halifax and will be accessed remotely by Symphony Services in Dallas. Access will only be made available during scheduled times and will be monitored by Government employees.</p>	<p>a. Symphony Services will not have the ability to remove or copy files. Once the conversion is complete, access will be disabled and only re-enabled during scheduled support services work. Symphony Services has read, understands and has signed off on <i>PIIDPA</i> obligations. Government employees on occasion may travel to Symphony Services offices to inspect the security measures used to protect personal information.</p>	<p>a. The EMS application was the best fit for the Telecom Service Group operational requirements. There were no cost-effective Canadian solutions available. Symphony Services has supplied the previous two telecom billing services, thus are familiar with the Provincial requirements. Their experience with migrating other clients to EMS lowers the Province's risks associated with migration of data. The EMS application server will provide a stable, secure operating environment. The Department</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>b. The Insurance and Risk Management (IRM) Group awarded the contract to supply and support the STARS software to CS STARS LLC, located in Chicago. STARS is used for claims management and insurance inventory by the Province. The data will be stored in Chicago and remotely accessed by IRM via a Halifax server.</p>	<p>b. CS STARS LLC has read, understands and has signed off on <i>PIIDPA</i> obligations. Government employees may travel to the CS STARS LLC offices to inspect the security measures used to protect personal information.</p>	<p>will be able to use the existing Oracle corporate licence agreement and will allow use of other current software that was not compatible with Tru Server.</p> <p>b. STARS fits the operational requirements of the IRM Group and there was no cost effective Canadian solution available. The Province has used the STARS system for 10 years.</p>
Agencies/ Boards/ Commissions	A (Description)	B (Conditions)	C (Reasons)
Film Nova Scotia	<p>Approximately four staff members traveled outside Canada on business. These staff members had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise e-mail system.</p>	N/A	<p>When staff is traveling outside of Canada for business reasons, they are expected to monitor their e-mail in order to fulfill their job responsibilities.</p>

Department	A (Description)	B (Conditions)	C (Reasons)
Utility and Review Board	Payroll details of Board members and staff were held by Ceridian Canada, a payroll service provider operating in Canada, but owned by a parent company resident in the United States.	Data was held as confidential records by the payroll service provider. Information was stored on servers located inside Canada.	Ceridian is the longstanding payroll provider for the Board. It was important to continue to hold the records until a suitable “all Canadian” firm could be located. That was done and the service converted in early 2008.
Nova Scotia Business Inc.	<p>a. Pursuant to s. 5(2) <i>PIIDPA</i> the head of Nova Scotia Business Inc. (NSBI) determined the storage/access outside Canada of business contact information in NSBI’s custody/control, as part of customer relationship management (CRM) data services supplied under contract by salesforce.com inc (a Delaware, US corporation with its principle place of business in San Francisco, California) is to meet the necessary requirements of NSBI’s operation.</p> <p>b. Pursuant to s. 5(2) <i>PIIDPA</i> the head of NSBI determined the storage/access</p>	<p>a. The business contact information is to be protected in accordance with the salesforce.com inc master agreement and privacy statement which recognize NSBI as owner of the stored data and provide strong privacy protection and security processes. The service is certified as a “Safe Harbour” under the EU Directive on Data Privacy and is certified “TRUSTe” privacy complaint.</p> <p>b. The personal information (primarily business contact</p>	<p>a. NSBI requires a robust and secure CRM platform to store and manage information necessary for the conduct of NSBI’s relationships with its clients, prospective clients, partners and stakeholders. The Salesforce® data service was selected through independent evaluation and based on its superior standing in meeting predefined objective evaluation criteria (including service functionality, IT compatibility, data security, vendor experience and cost). The tangible risk of compromising these critical service requirements outweighs the remote risk of business contact information (given its more accessible public nature) being the target of a foreign demand for disclosure.</p> <p>b. NSBI engages international in-market consultants as an essential and integral</p>

Department	A (Description)	B (Conditions)	C (Reasons)
	<p>outside Canada of personal information (primarily business contact information) in NSBI's custody/control, as part of the investment attraction and trade development services supplied under contract by international in-market consultants (global) is to meet the necessary requirements of NSBI's operation.</p> <p>c. Pursuant to s. 5(2) <i>PIIDPA</i> the head of NSBI determined the storage/access outside Canada of personal information in NSBI's custody/control, stored in, or accessed using, a mobile electronic device by an NSBI director, officer, or employee for business continuity purposes during international travel is to meet the necessary requirements of NSBI's operation.</p>	<p>information) is to be protected in accordance with the service agreement including confidentiality provisions.</p> <p>c. Personal information stored in or accessed using a mobile electronic device by an NSBI director, officer or employee during international travel is to have a reasonable and direct connection to the person's job duties and be protected by the director, officer or employee in accordance with the NSBI Code of Conduct and Oath of Office.</p>	<p>component of NSBI's trade development and investment attraction activities. The consultants are experts in the business environment within a business sector or geographic region of interest. International consultants operate from and travel outside Canada and must be able to store and access personal information (primarily business contact information) outside Canada in order to facilitate business connections/transactions in performing their contracted services.</p> <p>c. For business continuity purposes, NSBI directors, officers, employees must be able to store and access using a mobile electronic device personal information that has a reasonable and direct connection to the person's job duties so the person can perform work responsibilities while traveling outside Canada.</p>

Table 2: Summary of January 1, 2007 – December 31, 2007 Foreign Access and Storage by Health Authorities

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Annapolis Valley District Health Authority (AVDHA)	<p>a. The Pinestar Technology Inc. software maintenance contract was renewed for one-year</p> <p>b. It is estimated that 35 employees traveled outside of Canada for business and may have accessed personal information via laptop, Blackberry™ or PDA's.</p>	<p>a. N/A</p> <p>b. AVDHA has implemented encryption and passwords for laptops, Blackberry™ and PDA's.</p>	<p>a. N/A</p> <p>b. Current storage and access to personal information outside Canada is linked to existing programs, services and software utilized by AVDHA to ensure efficient operations.</p>
Capital District Health Authority	<p>Approximately three CDHA staff members traveled outside of Canada and may have (or had the ability to) access personal information via remote e-mail, Blackberry™, personal computer or by any other means. Note: this does not reference physicians who have CDHA privileges.</p>	<p>CDHA general information and sharing policies apply in this situation. More specific guidelines related to access and storage of personal information outside of Canada is under development.</p>	<p>Current storage and access to personal information outside of Canada is linked to pre-existing programs and systems utilized by CDHA and are deemed necessary for management and operations.</p>
Cape Breton District Health Authority (CBDHA)	<p>a. Approximately 25 employees traveled outside of Canada and may have accessed personal information via remote e-mail or Blackberry™.</p>	<p>a. N/A</p>	<p>a. N/A</p>

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	<p>b. CBDHA entered into seven application maintenance contracts with the following vendors: Toshiba Canada and G.E. Diagnostic for diagnostic imaging; Fresenius Medical for renal dialysis; Varian Medical and Ventana for radiation therapy, G.E. Diagnostics for EKG and Phillips Medical.</p>		<p>b. Current storage and access to personal information outside Canada is linked to pre-existing programs and systems utilized by CBDHA and are deemed necessary for ongoing operations.</p>
<p>Colchester East Hants (CEHHA)</p>	<p>Approximately three staff members traveled outside of Canada and may have accessed personal information via remote e-mail, Blackberry™ or Treo™ No contracts were renewed or signed during this reporting period.</p>	<p>Guidelines will be developed relating to access/storage of personal information outside of Canada once the regulations are released by the Department of Justice.</p>	<p>Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized by CEHHA and are deemed necessary in the ongoing operations of these systems and programs.</p>
<p>Cumberland Health Authority (CHA)</p>	<p>VPN access to Dictaphone System, Florida, for remote vendor application support. VPN access to Saturn OR system from US for remote vendor application support. Encrypted (SSL) staff access to CHA web mail system from US locations. Storage of information on whole disk encrypted CHA owned laptops.</p>	<p>Access to information stored on CHA networks and servers is only permitted through encrypted VPN connections. All external e-mail access is encrypted through SSL, VPN or the Blackberry™ service. The CHA has adopted a standard for encrypting all information</p>	<p>Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized in the CHA and are deemed necessary in the ongoing operations of these systems and programs.</p>

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		<p>on laptops and media that is released outside the CHA, including removable media such as encrypted USB storage devices and CD/DVD's.</p> <p>Established a process whereby all business changes that may affect the release, use or access to private information are reviewed regularly by the Privacy and Information Management committees. Privacy Impact Analysis must be completed on all new systems.</p>	
Guysborough Antigonish Strait Health Authority (GASHA)	Access to personal information outside of Canada is permitted only for the purpose of conducting GASHA business.	Vendors are required to follow <i>PIIDPA</i> legislation. Staff is required to follow GASHA's Privacy Policy.	Privacy Impact Assessments will be completed on new requests requiring remote access by Vendors. Decisions are made pending the outcome of this assessment. 24/7 access is not permitted.
Pictou County Health Authority	Access and storage from outside Canada is linked to pre-existing	Conditions or restrictions will be developed once the	No decisions were made on access to

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
(PCHA)	<p>programs and or systems utilized at PCHA which continue to be required to be used for the necessity in ongoing operation of these systems and programs (e.g., Meditech, Dictaphone, 3M). PCHA managers and senior leadership may have accessed their personal information while conducting business or vacationing outside the country using remote e-mail and Blackberry™.</p>	<p>regulations related to access/storage of personal information outside of Canada are released by the Department of Justice.</p>	<p>this information during this time period.</p>
<p>South Shore Health Authority (SSHA)</p>	<p>SSHA entered into several contracts that may require access or storage outside of Canada. 63 contracts are being reviewed.</p> <p>SSHA staff have been directed to refrain from the use of SSHA owned devices that contain personal information including Blackberry™ and cell phones while out of the country for pleasure or business. SSHA recognizes there may have been unauthorized access to information from outside the country using web mail or VPN. There was one out of country trip during the period January</p>	<p>The following clause now appears in all Requests for Proposals and Tenders awarded by SSHA: “Vendor acknowledges that in the performance of any Contract awarded hereunder it may obtain information concerning individuals which information is subject to protection in accordance with applicable legislation and regulation including, without limiting the generality of the foregoing, the <i>PIIDPA</i> Bill No. 19 and any other</p>	<p>Current storage and access to information outside Canada is linked to pre-existing programs/software used within SSHA and is deemed necessary for continued operations.</p>

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	1, 2007 to December 31, 2007	applicable Act or regulation. Vendor agrees to safeguard any such information in accordance with all such legislation /regulation and use same solely to comply with its obligations under the awarded Contract.”	
South West Nova District Health Authority (SWNHA)	<p>Several staff members traveled outside of Canada and accessed personal information via e-mail, web portal or Blackberry™. No decision has been made re the approval of access; however a tracking process has been established for managers.</p> <p>The following contracts are still under investigation re the ability to access personal information:</p> <ol style="list-style-type: none"> 1. Nova Industrial, one-year lease tank maintenance; 2. East Coast Capital, three-year IS equipment lease; 3. NS Environmental/Labour Elevator License – One year maintenance 	Developing an inclusion clause for contracts upcoming in 2008.	Access and storage from outside Canada is linked to pre-existing programs and/or systems utilized at the SWNHA, which are required for ongoing operations of these systems and programs.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	<p>4. Pinestar Technology Inc., one-year software maintenance – Nuclear Medicine;</p> <p>5. Carenet Service Inc. Electronic purchasing, one-year S-Care Net; and</p> <p>6. Hewlett-Packard.</p>		
IWK Health Centre	<p>a. 114 individuals (employees and physicians) made 121 work-related trips outside of Canada, as reported by costs centres that funded the travel. These numbers provide the number of out-of-Canada trips and not potential access to personal information. In circumstances where individuals travel with laptop computers or handheld devices, most access would be to e-mail. Remote access to other systems containing personal information is possible.</p> <p>b. In 2007 IWK had a version update to their Health Information System (Meditech). In order to complete the update the vendor requires access to the LIVE system. The IWK staff and</p>	<p>a. All information accessible remotely is encrypted.</p> <p>b. Storage or access to personal information outside of Canada by service providers and partners is done either under contract</p>	<p>a. N/A</p> <p>b. 1. The IWK has software/vendors located outside of Canada who maintain systems remotely. The IWK continues to use these vendors as these vendors provide a service which is required for</p>

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	<p>the vendor staff partnered to work through critical system issues to ensure the update is completed successfully and to ensure on-going performance of the update. Access by the vendor (Meditech, Boston) is always done through a secure dedicated connection. The information system logs vendor access by date and time. Access by the vendor is on request from the IWK.</p> <p>Contracts which provide for access/storage outside of Canada were reviewed for mitigation of access. If it was deemed that this access/storage was necessary, a confidentiality clause, secure network access and accountability were included in the contact and/or processes wherever appropriate.</p>	<p>with language addressing confidentiality or with consent of the individual.</p> <p>Conditions or restrictions related to access to personal information by employees while traveling outside of Canada will be developed to comply with the regulations once received from the Department of Justice. The IWK maintains a list of employees who traveled outside Canada on work related activities. While personal information is not taken by employees outside of Canada, some personal information may be accessible by employees through wireless handheld devices. When connecting to the IWK Communication system messages are encrypted while on route and all users of wireless handheld devices are encouraged to password</p>	<p>continued management and operations of the health centre. (Examples – Meditech, Boston which maintains health information system and Birthnet, Seattle, Washington – which maintains the Fetal Archiving System). Access to the systems is set out in written agreements and monitored by the IWK.</p> <p>b. 2. In circumstances where specialized laboratory testing is not available or cost prohibited in Canada, test resulting is done outside of Canada. When circumstances allow, consent is obtained. Laboratory services track external referral lab tests.</p> <p>b. 3. When the research sponsor is located outside of Canada, no personal identifiers are provided unless consent from the patient/legal guardian has been obtained.</p> <p>b. 4. A PIA (Privacy Impact Assessment) is requested when a new service is acquisitioned/implemented that requires transmittal or access to personal information outside the country or when a vendor is a</p>

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		protect their device.	<p>subsidiary of a US-based company. The PIA is reviewed by the Privacy Manger to ensure risks around disclosure of personal information are addressed.</p> <p>b.5. Certain on-going programs, which depend on treatment/patient care plans from US established groups obtain patient consent prior to transmittal of personal information. An example of these programs is the Children's Oncology Group (COG).</p>

Table 3: Summary of January 1, 2007 - December 31, 2007 Foreign Access and Storage by Universities

Universities	A (Description)	B (Conditions)	C (Reasons)
Dalhousie University	<p>a. Academic software: supports teaching activities and allows for online collaboration, e.g., voice, video, application sharing, etc. (storage in the US – plan to move to internal storage in 2008)</p> <p>b. Academic program: online plagiarism detection service (storage in the US).</p> <p>c. Student employment services program: online tool for a suite of products designed to</p>	<p>a. Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees.</p> <p>b. Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; storage of Dalhousie information will be segregated from other users. Internal security measures: process in place to minimize disclosure of personal information.</p> <p>c. Contractual security measures: restrictions on access to and disclosure of</p>	<p>a. Necessary for Dalhousie’s academic programs in a variety of disciplines; no Canadian product offers a comparable suite of products, service and functionality.</p> <p>b. Necessary for Dalhousie’s academic programs in order to maintain high standards of academic integrity. There is currently no product in Canada offering a comparable range of service and functionality. Minimal personal information disclosed.</p> <p>c. Necessary for Dalhousie’s student employment program. There is no service in Canada offering a comparable range of functionality.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p>assist students in seeking employment (storage in the US).</p> <p>d. Product warranty maintenance for electronics (storage in the US).</p> <p>e. Suite of analytical services to identify potential financial donors (storage in the US).</p>	<p>information by service provider and their employees; agreement in place to move storage of information from the US to Canada in 2008.</p> <p>d. Internal security procedures: Personal information provided is limited to what is necessary for warranty coverage; where possible and applicable, personal information will be removed from products sent to the service provider for maintenance or replacement.</p> <p>e. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees. When being transferred, information will be encrypted and sent via secure FTP.</p>	<p>d. Necessary for Dalhousie's program as a supplier of the service provider's products. Since the service provider is the exclusive supplier of maintenance under warranty, there is no Canadian alternative available.</p> <p>e. Necessary for Dalhousie's fundraising operations. Product is superior in terms of service and functionality.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p>f. Maintenance support for product which supports all major University administrative computing applications (remote access from the US or Bangalore, India).</p> <p>g. Maintenance support for product which allows University staff and faculty to schedule and manage meetings and activities in an integrated environment (remote access from the US).</p> <p>h. Maintenance support for facilities management product used for reserving</p>	<p>f. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.</p> <p>g. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.</p> <p>h. Contractual security measures: restrictions on access to and disclosure of information by service</p>	<p>f. Necessary service for the operation of integral Dalhousie academic computing services; no Canadian alternative identified; access rarely required.</p> <p>g. The ability to effectively schedule and manage meetings and activities are necessary for Dalhousie operations. This product offers superior functionality and range of service not identified in any Canadian alternatives; access rarely required.</p> <p>h. The ability to effectively manage room bookings through one centralized program is necessary for Dalhousie operations. This product offers superior functionality to the Canadian alternative, and there</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p>rooms on campus, specifically for events and classroom scheduling (remote access from the US).</p> <p>i. Maintenance support for student services product which allows faculty members to convey concerns to students about aspects of class performance and provide referral to on-campus resources (remote access from the US).</p> <p>j. Maintenance support by service provider who provides content management for Dalhousie web site and intranets (remote access from the US).</p>	<p>provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.</p> <p>i. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.</p> <p>j. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions,</p>	<p>would be a heavy cost to convert in terms of labour and acquisition costs; access rarely required.</p> <p>i. The ability to identify and address potential student performance issues at the earliest possible stage is necessary for the Dalhousie operations in terms of enhancing the student experience; no Canadian alternative identified; access rarely required.</p> <p>j. Keeping the Dalhousie web site current and functioning is essential to Dalhousie operations. Superior functionality; established service at Dalhousie; heavy cost to convert; access rarely required. Very limited amount of public personal information available.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p>k. Maintenance support for statistical software product, used in course teaching and research (remote access from the US).</p> <p>l. Maintenance support for academic product used extensively by faculty for online teaching (remote access form the US).</p>	<p>audit function, and pre-approved IP addresses.</p> <p>k. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.</p> <p>l. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-</p>	<p>k. Necessary for Dalhousie academic operations in several departments. This product offers superior functionality and range of service; access rarely required.</p> <p>l. The provision of online teaching is necessary to Dalhousie academic operations. This product offers a superior range of service and functionality; and has been an established service at Dalhousie for several years, therefore would require a heavy coast to convert; access rarely required.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p>m. Maintenance support for scheduling and data tracking software, designed for university student advising and counseling (remote access from the US).</p> <p>n. Maintenance support for a web-based database that manages information and processes related to student work experience placements in industry (remote access from the US).</p> <p>o. Maintenance support for product which</p>	<p>approved IP addresses.</p> <p>m. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.</p> <p>n. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.</p> <p>o. Contractual security measures: restrictions on</p>	<p>m. Providing advising and counseling services to students, and effectively managing and tracking those services, is necessary for Dalhousie student services operations. This product offers superior functionality and range of service; access rarely required.</p> <p>n. Effectively managing information and processes for student work placements is necessary for the operation of Dalhousie co-operative education programs, particularly in Architecture, Commerce, Computer Science, and Engineering. Cost prohibitive for Canadian alternative; access rarely required.</p> <p>o. Making calendars available on the wireless tools used by the faculty and staff who are required to</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p>allows for real-time synchronization of faculty and staff calendars with wireless tools.</p> <p>p. Maintenance support for academic product which provide students with information regarding their progress towards meeting their degree requirements (remote access from the US).</p>	<p>access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.</p> <p>p. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.</p>	<p>use them is necessary for Dalhousie operations. There is no suitable Canadian alternative, given Dalhousie IT architecture and costs to convert; access rarely required.</p> <p>p. Allowing students to access their information regarding progress towards degree requirements is necessary for Dalhousie operations, particularly in student advising and counseling, and for the Registrar's Office. No Canadian alternatives have been identified; access rarely required.</p>
University of King's College	Personal information about King's graduates and former students (name, address, employment, year of graduation or leaving King's, donations	King's will avoid retaining contractors that store personal information outside Canada, and will ensure personal information provided to a Canadian contractor for storage is not	Blackbaud Analytics provides this service for many Canadian universities and non-profit groups. The analysis was necessary to enable the King's Advancement Office to develop fundraising programs. King's sought legal advice before hiring Blackbaud and the contractor did not retain the

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p>history and relationships) provided to contractor, Blackbaud Analytics of Charleston, South Carolina to verify addresses and conduct a wealth assessment.</p>	<p>accessible outside Canada.</p>	<p>information.</p>
<p>St Francis Xavier</p>	<p>a. The University’s financial software “Bi-Tech” is provided by an American vendor, Sungard Bi-Tech (since 1988). This software requires periodic maintenance and updates. These maintenance needs are applied to our financial software through a remote access link between our server and a “Bi-tech” server located in Chico, California.</p> <p>The access to our server is for software</p>	<p>a. The university has taken steps to minimize our exposure to risk by restricting access to our system to designated and prescheduled time periods and only when maintenance and update activities cannot be accomplished by university personnel.</p>	<p>a. The cost of switching software vendors is prohibitive at this time. This is a mature software product and historically access has been for semiannual updates only, therefore we have minimal exposure points.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p data-bbox="531 269 835 524">maintenance and updates <i>only</i>, it is however theoretically possible that personal information could be accessed at those times, hence this notification.</p> <p data-bbox="531 602 835 1018">b. Established online alumni community through <i>imodules</i> in Kansas City that are based on their server. Records information has not been provided by the university, but rather is added by individual alumni who choose to do so.</p>	<p data-bbox="861 602 1228 898">b. Information added to the server program by our alumni becomes property of StFX University and is N/A or used by any other organization. Access is limited to graduates of Saint Francis Xavier University.</p>	<p data-bbox="1262 602 1917 670">b. This database was moved to a Canadian server in April 2008.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
Nova Scotia Community College	<p>NSCC has allowed for the storage of personal information under their control to be held by Apply Yourself Inc., Fairfax, Virginia. Apply Yourself is an application service provider offering web-based data management for the college's online application process. Will be reviewing alternate service providers in Canada. The College will provide disclosure to electronic applicants indicating that Apply Yourself Inc is an American company and the access and use of applications is subject to all federal, state and local laws.</p>		<p>The College will allow their employees to transport personal information temporarily outside Canada but only to the extent that it is strictly necessary for their assigned duties, or as a necessary part of a research project. This information will be transported using cellular telephones, wireless handhelds, laptops and storage devices. Employees will be required to take all reasonable precautions (e.g., encryption).</p> <p>The College will permit its employees to use web-based or other Internet access tools if it is a necessary part of performing his or her assigned duties or as a necessary part of a research project.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
Cape Breton University	<p>a. The University's Alumni/Donor Database, Raiser's Edge, is provided by an American vendor, Blackbaud located in South Carolina. While the software originates from Blackbaud, data is stored on servers housed at CBU. Blackbaud does also provide support service. If authorized by the University's software administrator, it is possible for the support technician to screen share site access. This access is restricted to the screen view only and controlled by the database administrator. Once the support is concluded, access is automatically terminated. This occurred only once in</p>	<p>a. Access to systems is restricted to authorized personnel only; access occurs only for the purpose of receiving technical support that cannot be accomplished internally.</p>	<p>a. The University's demand for requesting technical support is minimal to non-existent from year to year. Raiser's Edge software is fulfilling the needs of the University and the cost of purchasing new software is prohibitive at this time.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p>2007 for the purpose of receiving technical support.</p> <p>b. Approximately 65 CBU staff members traveled outside of Canada and may have (or had the ability to) access personal information via remote e-mail, Blackberry™, personal computer or by any other means. While traveling outside the country, such access is necessary for university administrators, researchers and other employees to perform their assigned duties or as a necessary part of a research project.</p>	<p>b. Access to information is authorized for the purpose of required assigned duties and research.</p>	<p>b. Storage and access as required to meet the operational requirements of the University.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
Nova Scotia Agricultural College	<p>The NSAC allows their Student Information System (SIS) provider, Datatel Inc., of Fairfax, Virginia, to provide Tier II application maintenance/support to their system, which is housed on the NSAC campus. No data resides in a foreign country. The SIS is utilized by a wide variety of stakeholders including students, staff, faculty, senior management, and various units/depts. (e.g., Financial Services, Registry, Continuing Education, Alumni Development and External Relations, Graduate Studies Office, Residence Services). The system houses all academic and student financial</p>	<p>Administrative rights are controlled by the NSAC Database Systems Administrator with username/password authentication for TCP/IP connectivity being granted to Datatel as required. This connectivity is restricted to a range of Datatel IP addresses. This access is monitored and compared to monthly reports provided by the vendor of the work that they have performed for the NSAC. Datatel's login information is periodically changed for security reasons and login information is only provided via direct communication via telephone to Datatel's head office.</p>	<p>When NSAC purchased the Datatel colleague/Benefactor system in 2004 there were no competitors in the Canadian marketplace. All three top SIS systems were provided by US vendors – this continues to be the case. Tier II support of this type of massive integrated system is typically provided by the vendor due to the breadth and depth of knowledge required for problem resolution. The vendor has a large staff that are highly trained consultants; systems support staff and programmers who are experts on the integrated system and its many components (client software, database, programming language, systems tools, etc.). The product is also always evolving and the university needs to maintain the ongoing relationship with the vendor to take advantage of enhancement as they develop. To properly complete daily business the NSAC must continue to have Tier II support provided by this vendor.</p>

Universities	A (Description)	B (Conditions)	C (Reasons)
	<p>account information, as well as alumni and campaign information. The SIS is a mission critical system that supports the core business activities of the NSAC.</p> <p>Datatel accesses the NSAC system on a monthly basis to solve problems that are not resolved by the NSAC first level of support which is provided by their in-house Database System Administrators. All access is via TCP/IP protocol. NSAC stakeholder access is restricted to internal NSAC network connectivity, while Datatel access is provided through firewall security to a restricted range of Datatel IP addresses.</p>		

Universities	A (Description)	B (Conditions)	C (Reasons)
	All TCP/IP and firewall/security management is provided by the NS Provincial Resources CSU – IT Division.		

Table 4: Summary of January 1, 2007 - December 31, 2007 Foreign Access and Storage by School Boards

School Boards	A (Decision)	B (Conditions)	C (Reasons)
South Shore Regional School Board	<p>a. Members of the Student Development Team authorized to access student records via laptop/modem when outside of Canada at conferences, for the purposes of managing student services case files. No other access authorized.</p> <p>b. Members of IT support staff authorized to access systems via laptop/modem when outside of Canada for the purpose of systems maintenance. No access of staff or student records involved. No other access authorized.</p>	Except for the cases noted in a. and b., no access of student or staff records of personal information is authorized.	<p>a. Student Development Team members may, from time to time, access electronic student records for the purposes of managing case files of student services cases.</p> <p>b. Ordinary maintenance of information technology systems requires technicians to access system files.</p>
Strait Regional School Board	a. There are online subscriptions for “United Streaming” and	a. The network allows secure VPN access only. More specific	a. Functionality of the operations of the Board are deemed necessary for management and operations.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	<p>“Reading A to Z” (education media). The teacher’s name and name of school are provided to both on-line education media providers.</p> <p>b. Forty-two (42) employees traveled outside of Canada and may have (or had the ability to) access personal information via remote e-mail, Blackberry™, personal computer or by any other means.</p>	<p>guidelines related to access and storage of personal information outside Canada.</p> <p>b. N/A</p>	<p>b. N/A</p>
<p>Annapolis Valley Regional School Board</p>	<p>Approximately five (5) staff members traveled outside of Canada and may have (or had the ability to) access personal information via remote e-mail, Blackberry™, personal computer or by any other means.</p>	<p>General information and sharing policies apply in this situation.</p>	<p>Access to personal information outside Canada may be linked to presently used programs and systems as part of the educational system and are deemed necessary for management and operations.</p>

School Boards	A (Decision)	B (Conditions)	C (Reasons)
Halifax Regional School Board	Two (2) staff members traveled outside Canada would have had access to personal information via their Blackberries™.	Relevant HRSB policies would apply to Blackberry™ usage outside of Canada. Each Blackberry™ is password protected. The HRSB will develop a policy related to access and storage of personal information outside of Canada.	One of the staff members at issue occupies a senior management position and must be available by e-mail for decision-making and information purposes. The other staff member occupies an administrative position and also must be available outside of Canada.

Table 5 - Summary of January 1, 2007 – December 31, 2007 Foreign Access and Storage by Municipalities

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
Halifax Regional Municipality	Seven (7) employees of Halifax Water traveled to Colorado for business purposes and did or potentially could have accessed personal information through use of their Blackberry™ or cell and one employee through the use of their laptop as well.	N/A	N/A
Municipality of the County of Kings	There was no permanent storage by third party contract of any kind, outside of Canada of personal information in the custody or under the control of the	Restricted access to corporate e-mail is available on authenticated login via username and password known only to the individual in question. Access to data is	The network security policy for the Municipality of the County of Kings requires strong passwords (minimum 8 characters including 2 non-alpha and 2 special characters with mixed case), as defined under network group policy and assigned by the corporate network administrator. Furthermore, the policy also mandates that any/all information being transmitted across the Internet with content deemed to be of a sensitive nature

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	<p>Municipality of the County of Kings. Access to data from outside Canada is restricted via the terms and conditions of the corporate network policy to authenticated login of authorized staff via portable computing equipment securely fitted and assigned to said staff as a means of securely communicating with home office for continuing business operations while traveling abroad.</p> <p>The aforementioned network policy is currently being revised to provide for sufficient advanced notice of staff travel plans so as to allow IT staff adequate time and access for the prior</p>	<p>available via network login using secure username and password over Virtual Private Network requiring authentication of the remote device as a permitted member of the corporate network. Per above, no storage of information by third party contract outside of Canada has been authorized.</p>	<p>(i.e., including names, addresses, etc.) must be transferred exclusively via VPN or using other encryption software as approved by the Manager, IT.</p>

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	inspection and removal of all personal information from systems accompanying staff traveling outside of Canada.		