Personal Information International Disclosure Protection Act

2011 Annual Report

NS Information Access and Privacy Office
October, 2012

Message from the Minister of Justice

I am pleased to provide the sixth 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 created to enhance provincial privacy protection activities and 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 public sector or municipal operations.

Under *PIIDPA* subsection 5(3), Nova Scotia public sector and municipal entities are required to report the decision and description of any foreign access and storage of personal information occurring from January 1, 2011 to December 31, 2011 to the Minister of Justice. This report is based on the *PIIDPA* reports received by the Nova Scotia Information Access and Privacy Office.

This report contains a summary of the 47 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. Note: 63 entities reported that there was no access or storage outside of Canada for the 2011 calendar year.

Original signed by the Minister

The Honourable Ross Landry

Minister of Justice and Attorney General

Contents

Key to Columns in 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: January 1 – December 31, 2011 Foreign Access and Storage by Government Departments, Agencies, Boards & Commissions [1]

Department	A (Description)	B (Conditions)	C (Reasons)
Agriculture	The Department started a YouTube channel for social media engagement not available on the government website. All YouTube channel content are also present on the Department website where information is neither stored nor is accessible outside of Canada so viewers can view the videos without personal information captured from abroad. Personal information collection from YouTube is voluntary. A user wishing to leave a comment needs agree to YouTube's conditions for getting one (email, user name, etc.) None of this is verified except for the email to make sure it is valid for use so no legally identifying personal information (i.e., real name, age, birth dates) has to be	All comments made on the YouTube channel are moderated for approval within 48 hours of comment being made before being allowed to be displayed publicly on YouTube with the video (if allowed). Moderation involves a wide range of criteria from language to sensitive information. Comments made, as well as information provided to YouTube to get an account to be able to comment, are stored on YouTube's server and accessible by YouTube. However, this is not any different from the process required of anyone to comment on any other YouTube video. YouTube staff, located in the US, have access to information submitted but YouTube has its own Privacy Policy to protect this information. Only very selected department staff have access to the Department YouTube Channel and will not access it from outside of Canada.	Any consideration for allowing storage or access of personal information outside of Canada would require the standard provincial government Privacy Impact Assessment to be done which needs approval by the Deputy Minister. Both the Department YouTube channel and the Growing Nova Scotia website had Privacy Impact Assessments done and approved by the Deputy Minister.

[1] Alcohol and Gaming , Economic and Rural Development and Tourism, Nova Scotia Health Research Foundation, Executive Council Office, Sydney Tar Ponds, Treasury Board Office, Policy and Priorities, Office of the Premier, Office of Police Complaints Commissioner, Office of Aboriginal Affairs, Waterfront Development, Nova Scotia Pension Agency, Nova Scotia Legal Aid Commission, Public Service LTD Plan Trust Fund, Nova Scotia Human Rights Commission, Public Service Commission and Environment reported that no personal information was accessed or retained outside of Canada.

Department	A (Description)	B (Conditions)	C (Reasons)
	given. The same requirements are also requested of millions of other YouTube users. IP addresses recorded by YouTube for access to the site only identify the Internet Service Provider used by the viewer, not identifying the viewer so that is not personal information. Given these small risks, many other government departments, levels and jurisdictions have also employed YouTube channels as an effective communications tool. Finally, a rigorous Privacy Impact Assessment (PIA) was done and approved by the Deputy Minister before the channel was created to identify proper usage, risks and mitigating measures. The Department also created a farmer investment website to help potential farm buyers find farms for sale in Nova Scotia (www.growingnovascotia.ca). Google Analytics is employed to monitor site traffic for determining main geographical locations with interest in its	The Growing Nova Scotia website does not present the real estate information in any format easier to manipulate than how it appears on the MLS site listings. All information is stored on provincial government servers in Nova Scotia. Because the information is meant to be accessible by anyone around the world, though, access to the real estate listings should not be limited.	

Department	A (Description)	B (Conditions)	C (Reasons)
	content for future marketing purposes. Google Analytics records IP addresses the Internet Service Provider through which a user accesses the site on Google's servers in the US. However, users cannot be specifically identified nor is any personal information given up. A database of farm property and owner contact is also used on the website which his meant to be used by people the world over. This information is publicly available on the MLS listing services website for real estate transactions in the same format. The data is only employed on the Growing Nova Scotia site for convenience and ease of usage for the user so as not to have to go back and forth between it and the MLS site. As a result, no greater risk is present in sharing the farm listing information.		
Chief Information Office	Symphony Teleca Corporation (Symphony) is under contract by the Province (PNS) to supply and support an Expense	A controlled remote access gateway allows Symphony to view the PNS database used by EMS to store personal information. However, it does not give	The EMS solution was selected by PNS because Symphony Teleca Corporation was the best option to ensure PNS telephone billing requirements could be

Department	A (Description)	B (Conditions)	C (Reasons)
	Management System (EMS). The EMS is used by the Chief Information Office (CIO) to track and manage telecommunication re-billing costs on a monthly basis. In the course of providing these contract services, Symphony occasionally requires remote access to the EMS application and database (stored at the PNS Datacentre) in order to perform scheduled support or troubleshooting activities. This access takes place from Symphony's offices located in Dallas, Texas using secure virtual private network software (also running on a server located in the PNS Datacentre). Each occurrence of remote access to EMS by Symphony is controlled and monitored by CIO staff.	Symphony Teleca Corporation the ability to remove or copy any files. Once Symphony Teleca Corporation's work is completed, its access to the database is disabled by CIO staff. Under the agreement with PNS, Symphony Teleca Corporation covenants that it will comply with its obligations as a service provider under PIIDPA and will strictly enforce the security arrangements required to protect personal information to which it has access. Symphony Teleca Corporation is also required to confirm the details of those security requirements upon receipt of a request to do so from PNS. PNS employees may at any time travel to the offices of Symphony Teleca Corporation to inspect the security measures it has put in place to protect such personal information.	met. Symphony Teleca Corporation's prior experience with other PNS telephone billing systems lowered the risk associated with support of the EMS system. There is currently no alternative method of receiving technical support access for EMS within Canada.
	Emergency and scheduled technical support access occur throughout the year for various vendor enterprise applications, software and hardware supported by the Chief Information Office (CIO),	The CIO maintains support contracts with these organizations to ensure that confidentiality of sensitive information is maintained. In most cases, the type of access required to resolve technical problems using remote access does not	Remote access to various networks, servers and storage systems supported by the CIO is strictly undertaken for the sole purpose of maintaining adequate technical support levels to service CIO client organizations. This remote access only

Department	A (Description)	B (Conditions)	C (Reasons)
	including Microsoft, Hewlett Packard, IBM, Barracuda Networks, Polycom Inc., Cisco, Dell, Novell, EMC, and Checkpoint Software. No storage of personal information is involved with these support connections and the access occurs over secure network connections monitored and controlled by CIO staff. These access events occur when CIO staff cannot resolve a technical issue and need to engage technical support resources from the various vendors to resolve the problem. Since many of these companies have implemented global support organizations, access usually occurs from the United States but can also be from countries such as Brazil, Israel, and India.	involve direct access to any personal information. In the rare cases that any access might be possible to personal information, the access is monitored and tightly controlled by CIO staff to ensure confidentiality is maintained. When remote access is required, it is controlled through a secure network connection that does not allow any direct data to be transmitted from PNS facilities to the remote vendor location. The remote access links can be monitored and disconnected at any time. In most cases, the access link must first be established by CIO staff to permit the vendor to initiate a remote connection. If, for any reason, sensitive information must be transmitted for troubleshooting or problem solving purposes, then it is sent through a secure and encrypted channel.	occurs with CIO staff involvement and monitoring. This type of remote access outside of Canada also only occurs when other support alternatives are not available. Only in rare circumstances is the transmittal of any personal information involved for these types of remote access connections. When required, strict controls are in place to ensure confidentiality is maintained at all times.
Communications Nova Scotia	Under the Province's privacy policy, Internet IP (Internet Protocol) addresses are considered personal information. For three internet-related initiatives, Nova Scotia Life, Pomegranate and Canada's	This information is subject to the Google Privacy Policy. (The Google Privacy Policy outlines its responsibility to protect any personal information it collects against any unauthorized access, disclosure or destruction. It further details that they will not share any	CNS is accountable in its business plan to report on the effectiveness of major Internet (and other) campaigns. Use of Google Analytics enabled us to collect and report on accurate statistics about how many visitors came to our website, from where and approximately how long they

Department	A (Description)	B (Conditions)	C (Reasons)
	University Capital, the CNS Marketing Division used a web statistical analysis service called Google Analytics that involved storing IP addresses on Google's servers in the US.	personal information without prior consent unless it is to comply with applicable laws. The equipment was accessed only by CNS employees.	stayed. This information allows us to refine our marketing and advertising strategies ensuring that we provide best value to the government.
	Six CNS employees travelled outside of Canada for business or pleasure with a cell phone, Blackberry and/or iPad.	All devices were password protected, except for one iPad, which was only used for work related communications to access GroupWise for email messages, post government Facebook account messages and use Twitter, which are all password protected.	The cell phone was needed to make and receive calls. Blackberries were necessary to make calls and use email. The iPads were used to email, post messages of Facebook and access Twitter.
Communities, Culture and Heritage	Nova Scotia Provincial Library (NSPL) maintains an integrated library system (ILS) on a cost-recovery basis for a consortium consisting of 64 branch libraries in eight regional library systems, and four government department libraries. The ILS provides a library catalogue, a purchasing module, and a circulation module (check-in/check-out, and client information). The ILS is mission critical for day to day operations	NSPL has implemented reasonable security measures to protect personal and other information in the ILS. The ILS software is maintained on a secure server in Brunswick Place. The contract with the company stipulates that NSPL staff must be contacted when the company requires access to the ILS server. NSPL enables SirsiDynix to access the server for specific upgrade activities at predetermined time periods, at the end of which SirsiDynix staff are logged out by NSPL staff. NSPL staff monitor and audit to ensure the access is	The decision was made to continue with SirsiDynix because there is no Canadian alternative. There are four major ILS vendors in the world that offer systems with the functionality required by libraries in the NSPL consortium, none of which are Canadian. When NSPL chose Sirsi in 2003, the company was a Canadian corporation. In 2005, Sirsi was purchased by Dynix, an American company, and became SirsiDynix. The company serves customers worldwide from its base in the United States.

Department	A (Description)	B (Conditions)	C (Reasons)
	of libraries. Without the ILS, libraries could not function.The ILS contains personal information about identifiable individuals (library clients in Nova Scotia), including name, address, telephone number and email address. This personal information is voluntarily given when a client registers for a library card. Attached to the clients' account number are titles currently on loan to the individual, those for which the individual has been billed and/or has paid and those which the user has requested. Transaction logs, maintained at NSPL, DOE, are retained for 3 months.The ILS is owned by an American Company, SirsiDynix, and access to personal client information from outside Canada is possible with SirsiDynix. There is no Canadian vendor which supplies a similar product.	reasonable and appropriate. SirsiDynix has no operational requirements to access personal information about clients. Due to these precautions, the risk of access to personal information about Nova Scotians by SirsiDynix is low, but it is technologically feasible.	
	Continued use of a Facebook page, titled 'Nova Scotia Museum'. Contents on page	N/A	In keeping with Direction 3 of the Heritage Strategy, to increase public recognition of the value and relevance of the province's rich heritage, the Promotions team has

Department	A (Description)	B (Conditions)	C (Reasons)
	consist entirely of Nova Scotia Museum Event listings and links to content on the Nova Scotia Museum websites, http://museum.gov.ns.ca. 'Find us on Facebook' link on the NSM parent website allows Internet visitors to view Facebook postings. Decision to implement Heritage Facebook and Twitter accounts entitled 'Nova Scotia Heritage', www.facebook.com/#!/novascotiaheritage, Contents on page consist of event listings and link to Heritage related content. The Heritage twitter account, titled 'Nova Scotia Heritage' is registered as https://twitter.com/#!/nsheritage. As above, the content is event listings and links to Nova Scotia Heritage related content. Continued use of a Twitter site, titled 'Nova Scotia Museum' and registered as http://twitter.com/NS_Museum. Contents on page consist entirely of Heritage - Nova Scotia Museum Event listings and links to content on the Nova		developed a marketing plan that includes developing a dynamic online presence; a key component of this plan is utilizing social media platforms to increase public recognition.

Department	A (Description)	B (Conditions)	C (Reasons)
	Scotia Museum websites, http://museum.gov.ns.ca. 'Follow us on Twitter Â»' link on the NSM parent website allows Internet visitors to view the Twitter feed without an account. Internet visitors can also view the NSM Twitter feed without a Twitter account using RSS.		
Community Services	1. The Department of Community Services signed a licensing agreement with the Consortium for Children of San Rafael, California, for the use of a home study methodology known as Structures Family Analysis Evaluation (SAFE). SAFE is copyrighted by the Consortium for Children, who own all rights to SAFE. As part of the licensing agreement, the Consortium for Children agreed to perform a yearly audit of files to enable quality control and identify staff training needs. Access to the home studies and supporting questionnaires completed by the staff of the Department of Community	1. Prior to forwarding the home studies and questionnaires, all identifying personal information was removed by staff of Community Services. Single initials remained to assist in the readability of the home studies. Only individuals assigned to the audit by the Consortium for Children were permitted access to the information from the home studies and questionnaires in order to accomplish the objectives of the audit. The Consortium for Children agreed that the home studies and questionnaires were to be considered confidential and proprietary to Community Services and the Consortium for Children agreed to hold the same in confidence. They have agreed not to use the confidential information other than for the purposes of the audit to enable quality control and	1. The Department of Community Services has ensured that no personal identifying information was shared, that the information was accessible only to authorized persons in order to meet the terms of the licensing agreement, that Consortium for Children held the information in confidence and that the information was securely stored on the premises of the Consortium for Children.

Department	A (Description)	B (Conditions)	C (Reasons)
	Services is necessary in order to fulfill the terms of the licensing agreement. A confidentiality agreement was signed with the Consortium for Children outlining the conditions placed on the storage and access of personal information outside Canada. 2. Since 2002, the Nova Scotia Housing Development Corporation has contracted Yardi Systems, Inc. under an alternate services provider (ASP) agreement to provide Tier II application support and maintenance as well as to manage the application hardware configuration necessary to operate the application. Tier II application support is provided by the Yardi Canadian offices operated in Mississauga, Ontario once issues reported are vetted by Housing Authority IT staff. The data is	identify refresher needs and to disclose the results only to the Manger of Adoption Services, Department of Community Services. The Consortium for Children agreed to return all copies of the home studies and questionnaires at the completion of the audit by courier and not to use the home studies for further training or demonstration. The Consortium for Children agreed that the home studies and questionnaires would be kept secure at its offices. 2. Under the terms of the contract, Yardi agrees that it will not 'use, disseminate or in any way disclose any of the confidential information' of the Nova Scotia Housing Development Corporation to 'any person, firm or business except to the extent it is necessary' to perform its obligations or exercise its rights.	2. Before entering into this arrangement, staff from the Housing Authorities (an agent of the Nova Scotia Housing Development Corporation) and the Department of Community Services underwent an RFP process and through a structured evaluation process of the proposals received, determined that the Yardi Systems software operated under an ASP agreement was the best solution. The software provided the best business functionality based on criteria defined at the time of the RFP process for the costs proposed. The technical framework proposed to operate this software was deemed acceptable based on criteria defined at the time of the RFP process for the costs proposed.

Department	A (Description)	B (Conditions)	C (Reasons)
	stored on database servers located at a Data Centre in Mississauga, Ontario operated by Q9 Networks. The application and database servers are managed by the Yardi Systems ASP Group located in Santa Barbara, California. This access is ongoing in order to ensure the ongoing operation and efficient performance of the server environment and the Yardi Voyager application, itself and minimize service disruptions to Housing Authority users. This group is also responsible for applying operating system patches and system upgrades as required. 3. Children in Care of the Minister of Community Services may require treatment services that are not available in the province, and on occasion, within Canada. During the 2011 calendar year, four children in care were placed in residential treatment facilities in the US to receive residential treatment	3. Information provided in these situations is to be used solely for the purpose of the determination of placement and the development of treatment plans for children.	3. Information provided to the placing facility is stored in accordance with the *Health Insurance Portability and Accountability Act (HIPPA)* of 1996. The information is stored in a locked environment on the facility campus for a period of not more than six years, or until the client reaches the age of 22, whichever is the longest. Information is released only with a written

Department	A (Description)	B (Conditions)	C (Reasons)
	services As part of the referral for placement to a treatment facility, information concerning the child, any medical diagnosis, treatment needs and relevant family information is shared with the placing facility. This information is provided to ensure that the facility will be able to meet the child's clinical needs and for the purpose of developing an appropriate treatment plan for the child. Information provided to the placing facility would include electronic information such as emails with agency social workers in Nova Scotia and paper copies of the information identified above.		request by the legal guardian or client, when the client has reached the age of 18 years.

Department	A (Description)	B (Conditions)	C (Reasons)
Education	1. The Provincial Student Information System (SIS) is used by the Nova Scotia education system (schools, school boards, Department of Education) to manage school operations, including processes such as student registration and enrolment, attendance, student scheduling, behaviour, student progress, individual program plans and school accreditation. In addition, the system is used to analyze and report on student achievement and other vital student, school and program data for policy and program decisions. The SIS contains personal information regarding students and parents, including names, addresses, phone numbers, email addresses, medical, behavioural incidents and academic records. This information about students and parents is necessary for the Nova Scotia education system to manage student enrollment and education from grade primary through high school.	1. The Department of Education has implemented reasonable security measures to protect electronic storage of personal and other information in the SIS. The information and software are maintained in a secure environment housed at the Department of Education, Brunswick Place, Halifax, NS. The contract with the service provider (Pearson School Systems) stipulates that Department of Education staff will authorize access to the environment by Pearson technical staff located in Rancho Cordova, California, USA, for the purpose of providing periodic technical support. Such access will be limited to predetermined time periods, at the end of which access is terminated by Department staff. Staff monitor and audit to ensure the access is reasonable and appropriate. Pearson has no operational requirements to access personal information about clients. Therefore, the risk of access to student and parents' personal information by Pearson is low, but it is technologically possible.	1. The decision to contract with Pearson for provision of the Student Information System was reached after an extensive evaluation of vendor products through a tendering process. Pearson was chosen due to its superior functional capability in meeting the requirements of the Nova Scotia education system as well as its standing as a leading distributor of Student Information System software worldwide.

Department	A (Description)	B (Conditions)	C (Reasons)
	2. The Teacher Certification Fee Processing service enables teachers to pay online for certain teacher certification services. The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the United States for payment authorization and reconciliation. Personal information that is transmitted through or stored outside Canada is at risk of a foreign demand for disclosure.	2. The Online Payment System has been developed in adherence with government and departmental security standards to ensure system access is restricted to authorized individuals and information is protected against unauthorized disclosure. Cardholders have agreed to the card issuing institutions' privacy statements that include a notice that third party service providers may be used to process credit card transactions.	2. Teacher Certification offers the option of payment by credit card payments as a convenience for teachers, and to provide efficient and effective online services.
	3. A number of Department of Education staff traveled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in GroupWise email system, using devices such as the BlackBerry and laptops.	3. Remote access to staff email accounts through web access to GroupWise is protected by username/password authentication and is delivered over an SSL-encrypted link via the secure BlackBerry GroupWise server.	3. Staff are sometimes expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. BlackBerrys were necessary to make calls, access email and Internet sites, and make telephone calls. Laptops are needed for preparing document, and accessing email and Internet sites.
	4. Teacher Summer Professional Development Registration System permits payment for	4. The Online Payment System has been developed in adherence with government and departmental security standards to ensure system access is restricted to	4. The option of payment by credit card payments is a convenience for teachers,

Department	A (Description)	B (Conditions)	C (Reasons)
	services using a credit card. The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the United States for payment authorization and reconciliation. Personal information that is transmitted through or stored outside Canada is at risk of a foreign demand for disclosure.	authorized individuals and information is protected against unauthorized disclosure. Cardholders have agreed to the card issuing institutions' privacy statements that include a notice that third party service providers may be used to process credit card transactions.	and provides efficient and effective online services.
Energy	Staff traveling outside of Canada may have taken electronic devices including Blackberries and laptop computers which may store and/or access personal information.	Remote access to staff e-mail accounts through web access to GroupWise is protected by username/password authentication and is delivered over an SSL encrypted link via the secure Blackberry GroupWise server.	When staff travel for work related matters, they may need to carry electronic devices (e.g., Blackberries, laptops) in order to monitor email and/or conduct business for operational purposes.
Film Nova Scotia	Approximately two staff members traveled outside Canada on business. These staff members had the ability to access personal information carried on email or stored in GroupWise via remote access to the GroupWise email system.	N/A	Staff, travelling outside of Canada for business reasons, are expected to monitor their email in order to fulfill their job responsibilities.

Department	A (Description)	B (Conditions)	C (Reasons)
Finance	1. Royal Bank of Canada (RBC) was awarded a contract in 2010 by the Province of Nova Scotia to provide electronic vendor payments to US vendors/individuals for the period 2011 to 2013.	1. RBC has entered into a service agreement with the Province of Nova Scotia. The terms set out consider the automated clearing houses (ACHs) required to process electronic vendor payments outside Canada. RBC are required to report to the Minister of Finance all unauthorized access or foreign disclosure of personal information. All Automated Clearing House (ACH) Payments are governed by the National Automated Clearinghouse Association (NACHA) because of the sensitivity of the data on the files. Use of ACH data for purposes other than to affect the transfer of the funds is not endorsed by NACHA and in some cases may be illegal. Each bank in the US must comply with the rules of NACHA. Vendors opt into receiving electronic payments. They are required to complete an application form, consenting to have payments forwarded to them via our electronic vendor payment (EVP) system.	1. Electronic vendor payments provide a low cost, flexible and highly reliable payment system to vendors. The requirement to electronically forward funds to vendors located in the US requires that information flows through an Automated Clearing House. There is no ACH that stores information in Canada.
	2. Remote Access via Blackberry. There were four instances that staff members were approved to take their Blackberry while travelling	2. Permission must be granted in order to take a Blackberry out of the Country. Remote access to email is protected by username/password authentication and is	2. When staff travel they may be required to conduct business or maintain contact with operations.

Department	A (Description)	B (Conditions)	C (Reasons)
	outside Canada and may have accessed personal information contained in email via Blackberry. 3. The Department of Finance operates SAP systems for the public sector including provincial departments, school boards, regional housing authorities, district health authorities, IWK Health Centre, Nova Scotia Liquor Corporation and several municipal organizations. It is necessary that remote access to public sector SAP systems be performed by SAP support staff via secure network connections to provide routine and emergency support maintenance. Following a highly audited and controlled management approval process, access to SAP systems occurred several times throughout the reporting period as required to correct or troubleshoot various problems within the SAP systems. Access was only from SAP's own secure internal support network	delivered over a secure server link (SSL) encrypted link. All Blackberries must be password protected. 3. When SAP support staff have reason to access any of the Province's SAP systems as a part of problem remediation, all production system transaction access is approved by CIS Division management and all access activity is recorded in an audit log so that verification can be done of whether personal information has been accessed. In addition, this access occurs over secure network connections that must be opened to allow SAP to enter a specific system. This secure network connection also prevents other parties from gaining unauthorized access to the SAP systems. This type of remote access very rarely involves actual access to personal information and is typically limited to system operations information. In cases where approved access does involve potential access to personal information for the purposes of resolving a specific support problem, records and audit logs of that access are maintained. In all cases where access was granted to SAP support staff, specific controls on the time and duration of that access are	3. 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 access to SAP systems permitted without the knowledge and approval of CIS 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 negate the need for 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.

Department	A (Description)	B (Conditions)	C (Reasons)
	and carried out by SAP staff resident in SAP service locations such as the United States, Ireland, Brazil, Germany and India. 4. Remote access staff members who traveled outside Canada may have had the ability to access personal information contained in email via remote email by personal computer.	maintained. There is no storage of data from SAP systems outside Canada. 4. Remote access to e-mail is protected by username/password authentication and is delivered over a secure server link (SSL) encrypted link. TS web access control software is protected by username/password authentication.	4. When staff travel, they may be required to conduct business or maintain contact with operations.
Fisheries and Aquaculture	None	None	No decisions were made to allow storage or access of personal information outside of Canada in 2011. Any consideration for allowing storage or access of personal information outside of Canada would require the standard provincial government PIA to be done which needs approval by the Deputy Minister.
Halifax-Dartmouth Bridge Commission	Halifax-Dartmouth Bridge Commission's (HDBC) MACPASS software application maintenance and support is provided by VESystems located primarily in Irvine, California. VESystems provide both routine	Access is controlled through a secure virtual private network and services provided for are per terms set out in an annual service agreement.	The MACPASS back office software application is a proprietary software application that is critical to HDBC and its ability to conduct and operate its electronic toll collection program. The system was purchased in 2008 and has been maintained by its developer, VESystems, since

Department	A (Description)	B (Conditions)	C (Reasons)
	maintenance and upgrades and thus have access to personal information through a portal to HDBC's internal network. Access is fairly routine and would occur minimally once a month.		implementation.
Halifax Regional Water Commission	1. Thirty-two staff were permitted to transport personal information devices, such as laptop computers, cell phones, and electronic data storage devices outside 58 times. 2. The following vendor, Tokay Navigator Software, Framingham, Massachusetts, provides initial customer data conversion and upload, periodic software maintenance and upgrades and customer technical support.	1. Prior to travelling, staff were advised that Halifax Water communication tools (cell phones, blackberries, laptops, memory sticks, VPN) are to be used for operational requirements only and were to be password protected. 2. Vendor access is controlled through a secure network portal (no direct link to support customer account information located in SAP). Customer technical services are provided for in the annual agreement.	1. Halifax Water staff were approved for travelling outside Canada with their communication device(s) to ensure they remained in contact with other utility staff to fulfill operational responsibilities. 2. Vendor access is crucial to manage the Cross Connection Control Program.
Health and Wellness	**<u>Storage</u>** There were no approvals granted for the storage of personal information in the		

Department	A (Description)	B (Conditions)	C (Reasons)
	custody or control of the Department of Health and Wellness outside of Canada for 2011. **Access** The Department of Health and Wellness granted the following approvals for access to personal information in the custody and control of the Department outside of Canada for 2011: **McKesson Corporation, STAR Patient Processing** The McKesson STAR Patient Processing system is the patient admission tool currently implemented in the Capital District Health Authority (CDHA). McKesson will be enhancing CDHA's patient admission tool to support the provincial Electronic Health Records (EHR or SHARE's (Secure Health Record) integration requirement for patient active admissions, discharges and transfers. The	**McKesson Corporation, STAR Patient Processing** McKesson developers need to access the local provincial Client Registry from their offices outside of Canada to deploy the software changes and test the enhanced software with the provincial Client Registry. The Client Registry data will not be stored outside of the country. McKesson's development staff will use a pre-existing secure 'data tunnel' to connect the McKesson test system to the provincial Client Registry test system to complete the enhancement testing. The provincial Client Registry is located in the HITS-NS data center. All users	**McKesson Corporation, STAR Patient Processing** McKesson will be enhancing CDHA's patient admission toll to support the provincial Electronic Health Records (EHR) or SHARE's (Secure Health Record) integration requirement for patient active admissions, discharges and transfers. The McKesson product used to register patients in CDHA is proprietary to McKesson so no other vendor can perform the changes. The McKesson code and product development site is located in the United States.

Department	A (Description)	B (Conditions)	C (Reasons)
	software vendor, McKesson, is developing, testing and implementing the software changes needed to supplement the CDHA registration through use of the provincial Client Registry data. McKesson developers need to access the local provincial Client Registry data. McKesson developers need to access to local provincial Client Registry from their US based offices to deploy the software changes and test the enhanced software with the provincial Client Registry. The Client Registry data will not be stored outside of the country.	accessing the data will require security sign-on to the Star-Patient Processing system and will need to be given access to the provincial client registry integration by the hospital IT staff. Select McKesson developers/testers will have access to the test system. McKesson developers/testers will be pre-approved and must sign a confidentiality agreement. McKesson developers/testers access will be terminated immediately at test completion which is forecast for April 30, 2012. No personal information will be downloaded or copied by McKesson. All requests into the registry will be tracked and audit reports provided for review. McKesson Corporation is committed to following all Health Insurance Portability and Accountability ("HIPAA") regulations and all Ministry requirements for protecting patient information in Canada. HIPAA is United States federal law which includes provisions for the protection of privacy of certain individually identifiable health information referred to as protected	

Department	A (Description)	B (Conditions)	C (Reasons)
	FairWarning FairWarning is an appliance based application that facilitates the creation of privacy audit reports for health information systems. The FairWarning tool allows audits to be conducted of user access to electronic health information systems. FairWarning staff require access from outside of Canada to assist in the set up and ongoing maintenance of the FairWarning application; this includes having access to the application audit log database that contains limited personal information. FairWarning may also assist in providing FairWarning application training to District Health Authority Privacy Leads and other appropriate DHA/Department of Health and Wellness/HITS-NS staff using the application and audit log	health information. **FairWarning** The Master Agreement with FairWarning prohibits storage or access of personal information outside of Canada unless the Department consents in writing. FairWarning's development staff will use a pre-existing secure 'data tunnel' (VPN) to connect to the information stored on the appliance server to complete the configuration and testing of reports. The appliance server is located in the provincial data centre. Select FairWarning project managers/developers/testers will have access to information. No personal information will be downloaded or copied by FairWarning. The FairWarning appliance keeps a log of all access to appliance/application. The vendor will also inform HITS-NS when they access the server to perform maintenance. Access logs will be reviewed for compliance. No patient data will be downloaded or copied from the appliance. FairWarning Corporation is committed	**FairWarning** The FairWarning application will be used to augment current user access audit approaches for various provincial health information systems. FairWarning is an appliance based application that facilitates the creation of privacy audit reports for health information systems. The FairWarning tool allows audits to be conducted of user access to electronic health information systems. The application will be used to augment current user access audit approaches for various provincial health information systems.

Department	A (Description)	B (Conditions)	C (Reasons)
	data. **Relay Health** McKesson Canada, operator of the Department of Health HealthLink811, partnered with Relay Health to develop their Telecare application. As a result, Relay Health provides third level technical support for the information technology application that enables HealthLink811 operations. In cases where third level technical support is needed for the Telecare application, Relay Health, a US based company, will require remote access to the	to following all Health Insurance Portability and Accountability ("HIPAA") regulations and all Ministry requirements for protecting patient information in Canada. HIPAA is United States federal law which includes provisions for the protection of privacy of certain individually identifiable health information referred to as protected health information. **Relay Health** Access is temporary and only utilized when required after IT support at the work station and levels through the call centre are unable to resolve. To ensure the security of personal information, access is granted through a secure VPN. Access will be granted to the Implementation Engineer, the Development Team or the 24 hour Technical Support Analyst as required. While access to the CECC means Relay Health have access to personal information stored in Canada, the scope and focus of access rights will be limited to the source code of the application. Policies and procedures dictate that at no time shall Relay Health download or copy information from the CECC. The	**Relay Health** McKesson Canada's partner in the development of the Teletriage application is Relay Health. As a result, Relay Health is the only available provider of third level technical support for the information technology application that enables HealthLink811 operations.

Department	A (Description)	B (Conditions)	C (Reasons)
	CECC which contains personal information from outside of Canada. **<u>Language Line Services</u>** Language Line Services was subcontracted by McKesson Canada to provide telephone based language interpreter services for callers whose first language is not English. Language Line Services are provided by multiple sources across North America. Access to personal information is granted through obtaining consent from the caller to engage third party interpretation services to facilitate the call in the caller's language of choice. **<u>DOH Employee Access</u>**	CECC is monitored by McKesson and all downloads are print activities are captured through the change control system employed by McKesson. As well, employees of Relay Health, under the umbrella of McKesson Corporation, are bound by the Corporate Code of Conduct. **<u>Language Line Services</u>** The interpreter service is provided over the phone. Language Line services, as per McKesson's policy requirements, do not result in downloading, printing or documentation of personal information. Interpreters trained in language interpretation are the only representatives who have access to personal information through the encounter. **<u>DOH Employee Access</u>** The Department of Health and Wellness *Transmission of Confidential*	**<u>Language Line Services</u>** McKesson Canada has entered into a partnership with Language Line Services to meet contractual requirements for the provision of culturally safe care and improving access to primary health care services for all Nova Scotians. This third part interpretation service is required to address linguistic barriers. McKesson Canada identified they would be unable to meet the service level standards outlined in the contract if they used the known Canadian service – CanTalk. **<u>DOH Employee Access</u>** When staff are traveling for business reasons (e.g., meetings, conferences), they are expected to monitor their email and

Department	A (Description)	B (Conditions)	C (Reasons)
	Thirty-eight staff of the Department of Health and Wellness 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.	*Information by E-mail and Fax Guideline (2004)* prohibits the inclusion of personal information in email sent outside the GroupWise system unless the email is encrypted and password protected. The Guideline also recommends limiting the inclusion of personal information contained in email within the GroupWise system. Therefore, the amount of personal information held or sent by email and, therefore, available for access while staff were outside the country, should be limited. All Blackberry devices issued by the Department are automatically password protected.	voice mail where possible. Therefore, it is necessary for them to check email remotely, where possible, in order to fulfill their responsibilities.
In*NOVA*Corp	There were 10 employees who travelled for business or pleasure and through those 10 employees; there were 29 different acts of access, which included VPN access, Blackberry access and or webmail access. Most activity occurred within North America	VPN, blackberry and/or webmail access usage is password protected either through an individualized password or a company set password. Both types of passwords are changed on a regular schedule. Other items listed above require individual password sets are and changed on a regular basis.	For business continuity and maintenance, Innovacorp senior management and other key staff must be able to store and access information using various mobile and electronic devices, as long as there is reasonable and direct connection to the person's job duties while travelling outside Canada.

Department	A (Description)	B (Conditions)	C (Reasons)
	but access was also made in the UK and Mexico. In addition, Innovacorp uses the following during the normal course of business IBM Global Services expense management platform Jan 1, 2011-Dec 31, 2011WebEx Jan 1, 2011-Dec 31, 2011 Web conferencing purposes Surveymonkey Jan 1, 2011-Dec 31, 2011 Employee survey purposes Skype Jan 1, 2011-Dec 31, 2011 Web conferencing purposes Facebook Jan 1, 2011-Dec 31, 2011 Social marketing purposes Twitter Jan 1, 2011-Dec 31, 2011 Social Marketing purposes Slimtimer Jan 1, 2011-Dec 31, 2011 on-line tracking purposes.		
Intergovern-mental Affairs	In 2006, the department entered into a service contract with Iron Mountain Canada Corporation (a Canadian subsidiary of Iron Mountain Incorporated) for the storage of paper records which are not accessed regularly but are not ready for storage at the Government Records Center. The offsite storage/retrieval/	Iron Mountain is to contact Intergovernmental Affairs upon receipt of a subpoena or similar order unless such notice is prohibited by law. Confidential information shall be held in confidence by Iron Mountain and shall be used only in the manner contemplated by the agreement. Iron Mountain shall use the same degree of care to safeguard the confidential information of	This decision was made to address the issue that Intergovernmental Affairs has limited space while at the same time business activities create records that remain relevant for long periods of time. Iron Mountain specifically was chosen because, at the time, no Canadian owned competitor in Nova Scotia could be found. Furthermore, they are considered to be their industry lead. Since 2009,

Department	A (Description)	B (Conditions)	C (Reasons)
	shredding vendor is a subsidiary of a US based company. The information is not transferred outside of Canada. While Intergovernmental Affairs has been systematically withdrawing records from Iron Mountain, some records are still held there.	Intergovernmental Affairs as it utilizes to safeguard its own confidential information.	Intergovernmental Affairs has been systematically withdrawing its records from Iron Mountain and transferring them to the Government Records Centre. Intergovernmental Affairs is currently unable to transfer large volumes of records to Records Centre due to it being filled to capacity. As a response to this, Intergovernmental Affairs is striving to identify records which may be eligible for archive to bypass Records Centre and also is seeking to free up storage space in the Intergovernmental Affairs Central Registry to store the records on site until space at Records Centre becomes available.
Justice	**A. <u>Travel.</u>** Seventeen staff members of the Department of Justice travelled outside out of the country during 2011 with a Blackberry, Laptop or other electronic device that contained personal information (work related). **B. <u>Correctional Services</u>** After reviewing proposals responding to an RFP, it is clear that there were no qualified companies who could offer a	**A. <u>Travel.</u>** Employees are expected to maintain communication with staff at the office and ensure that their Blackberries and laptops are password protected and that the Government server (which is encrypted) is utilized. **B**. **<u>Correctional Services</u>** 1. JEMTECS' Project Manager and the Provincial Electronic Supervision Coordinator shall be the only persons authorized to establish user accounts	**A. <u>Travel.</u>** Blackberries, laptops or other electronic devices were utilized to maintain contact with their offices and to communicate with staff while out of the country. **B. <u>Correctional Services</u>** This access is necessary to ensure optimal service and to maintain automated monitoring systems that communicate system issues such as hardware failures,

Department	A (Description)	B (Conditions)	C (Reasons)
	system which would store data only in Canada. JEMTEC Inc. was awarded the contract for Electronic Supervision of Offenders. All personal information is stored in secure data bases located in secure Monitoring Centres owned/operated by JEMTEC (including its subcontracted monitoring services), BI and Any Transactions Inc., located in Toronto, Ontario, Canada, Boulder, Colorado, US and Decatur, Georgia, US respectively.	(logins and passwords) for the host monitoring system. 2. Only JEMTEC Inc. and DOJ personal, designated by the NS DOJ, shall have 'permanent' user access to the host monitoring system. JEMTECS' Project Manager shall immediately notify NS DOJ 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, specific data compromised and duration of the access. JEMTECS' Project Manager shall verify what steps have been taken to prevent further unauthorized access. 3. The system 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	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.

Department	A (Description)	B (Conditions)	C (Reasons)
		purposes. Access to the system is via a standard internet browser with 128 bit SSL encryption with predefined timeouts to lock out users are periods of inactivity after they have logged in for security purposes.	
	C. <u>Legal Services</u>. **1.** The litigation lawyers and administrative staff use a document management program called Practice Manager to store all case material. While the database is stored on DOJ servers, from time to time when there is an issue with the program, DOJ contacts the provider Automon, which is a US company, and to resolve the issue they conduct a live meeting in order to access the computer and program to see what's going on. 2. Under the Child Abduction Act, c. 67, R.S.N.S., 1989, implemented the Hague Abduction Convention. Personal information relating to parents,	**C. <u>Legal Services</u>**. 1. Information is stored or accessed outside of Canada in compliance with contract. 2. Restrictions or conditions as per Hague Abduction Convention.	2. Child Protection Group at DOJ required to disclose information as part of the duty imposed by the Convention for

Department	A (Description)	B (Conditions)	C (Reasons)
	grandparents and children was shared with Agency Authority (Washington) in USA and child protection agency in Georgia for court application. **D. <u>Maintenance Enforcement Program (MEP)</u>** The Director of MEP has an obligation, pursuant to the *Maintenance Enforcement Act*, to enforce all maintenance or support 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 *Maintenance Enforcement Act* to disclose personal information to a reciprocating jurisdiction for the purpose of enforcing a filed maintenance order. The Director is also required to enforce maintenance or support orders which have been	**D. <u>MEP</u>** If the Payor of support resides outside the Province, the Director may be required to send personal information to the jurisdiction in which the Payor resides, if that jurisdiction has been declared a "reciprocating jurisdiction" under the regulations made pursuant to the *ISO Act*. 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 *ISO Act*, 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.	Nova Scotia for court application. **D. <u>MEP</u>** The Director is also required to send personal information to reciprocating jurisdictions in order to comply with the statutory obligations and duties under the *Maintenance Enforcement Act.* The Designated Authority is required to send personal information to reciprocating jurisdictions in order to comply with its statutory obligations and duties under the *ISO Act*.

Department	A (Description)	B (Conditions)	C (Reasons)
	registered for enforcement in Nova Scotia, under the *Interjurisdictional Support Orders Act* (*ISO Act*), by, or on behalf of, support recipients who reside outside the Province, in the reciprocating jurisdiction. The Designated Authority (Court Services), designated by the Minister of Justice pursuant to the NS *Interjurisdictional Support Orders Act* (*ISO Act*), sends personal information 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 *ISO Act*. The personal information sent by the Designated Authority outside Canada is the personal information which is contained in the documents that are		

Department	A (Description)	B (Conditions)	C (Reasons)
	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 *ISO Act*, to thereupon transmit or send these documents to the reciprocating 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. **E. <u>Iron Mountain</u>.** In July 2004, the Department of Justice entered into a service contract with Iron Mountain Canada Corporation to provide	**E. <u>Iron Mountain</u>**. Information held in a confidential and secure manner as outlined in agreement with Iron	**E. <u>Iron Mountain</u>.** The Department of Justice entered into this contract as there

Department	A (Description)	B (Conditions)	C (Reasons)
	document destruction and government record storage. In 2005, the Department of Justice reviewed the physical and procedural security and access environment at Iron Mountain Canada Corporation in Hammonds Plains. In 2011 there were 1800 cartons of DOJ records stored with Iron Mountain in Bedford.	Mountain.	was insufficient storage available at the Records Centre.
Labour and Advanced Education	1. There were approximately 5 departmental employees who traveled outside Canada with a Blackberry electronic device with some contact information, for departmental operational purposes, who may have accessed personal information through email. 2. Labour & Advanced Education utilizes NRSPro.com (formerly GEDScoring.com) software for the purpose of storing and processing information, in support of the General Educational Development (GED) program. The GED is composed of a	1. Authorization for traveling across international borders with these electronic devices was authorized by the Deputy Minister in all cases in keeping with government policy and protocol. 2. The department has a contract with NRSPro stipulating 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 with access to store and retrieve Nova Scotia	2. In November 2001, an evaluation of options for delivery of the GED program was completed. It was determined that there were only two vendors (OSS & NRSPro) certified by GEDTS to conduct test scoring that the department felt confident would be able to handle Canadian requirements. Both vendors were application service providers (ASPs)

Department	A (Description)	B (Conditions)	C (Reasons)
	series of five tests that evaluates participants' skills and knowledge in the areas of Language Arts Reading, Language Arts Writing, Mathematics, Social Studies and Science. The GED is an internationally recognized assessment tool of high school equivalency. The GED credential is accepted by employers across Nova Scotia and Canada and serves an important function for labour mobility. The GED tests are designed to measure the skills that correspond to those of recent high school graduates. The tests involve the ability to understand and apply information; to evaluate, analyze, and draw conclusions and to express ideas and opinions in writing. Adults who pass the five tests receive a Nova Scotia High School Equivalency certificate of Grade 12. There are approximately 1,500 tests conducted each year in Nova Scotia. The department scans the test	information. This transmission is over a SSL connection using an encrypted link. The test results and certificates are also available for viewing by authorized departmental staff on the NRSPro web site using the same security methods. A user ID and password are also required for access. The department scans the test sheets locally and sends data to NRSPro over an encrypted Secure Sockets Layer (SSL) connection. The information is stored in a database at NRSPro located in Spanish Fork, Utah, USA, for processing and as a record for future reference. Continued storage is required for data retrieval and combining of score results for students rewriting tests that were not passed successfully. In the event the department terminates services with NRSPro, the data will be returned /transferred to the department or another service provider and removed from the NRSPro database.	located in the USA. The 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. The other option available to the department 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 which would have resulted in an interruption in client service to allow time to design the system and obtain certification from GEDTS. In 2001, the department's decision was made to contract with OSS (Oklahoma Scoring Service based in Norman, Oklahoma, USA) for the 2002 GED test series, based on their extensive experience in GED test scoring, maturity of the software solution, security methods in use for transmission of information, and high reputation across educational jurisdictions. In addition, OSS came highly recommended by GEDTS. In July, 2009, the department terminated our contract with OSS and began working with NRSPro.com. Data was transferred to our new service provider, NRSPro. NRSPro had been the department's scoring service provider from 1993 to

Department	A (Description)	B (Conditions)	C (Reasons)
	sheets locally and sends data to NRSPro over an encrypted Secure Sockets Layer (SSL) connection. The information is stored in a database at NRSPro located in Spanish Fork, Utah, USA for processing and as a record for future reference. Continued storage is required for data retrieval and combining of score results for students rewriting tests that were not passed successfully. The test scoring is completed remotely by NRSPro and the test results and certificates are transmitted to the department in PDF files to be printed locally. The information is transferred by NRSPro to the General Educational Development Testing Services (GEDTS) international database. The international database contains information used for statistical reporting of GED achievements by jurisdiction. The database includes gender, age, country, province, number of participants, number passed, number failed, etc. GEDTS is		2001, prior to the release of the 2002 test series and the new technical scoring requirements (uploads to the IDB). The decision to switch to NRSPro came from polling other Canadian provinces. It was determined that NRSPro provided an overall better service including instant scoring and immediate reporting times, detailed reports, incorporating NS forms and letters as report options and allowing students and third-party verifiers to get instant results online.

Department	A (Description)	B (Conditions)	C (Reasons)
	located in Washington D.C., the international database is housed by Marsys, a service provider located in Miami, Florida with a backup database maintained at their office in San Mateo, California. Marsys have a contract with GEDTS for support and management of the GEDTS international database. The international database was established in support of the GED program and it is mandatory that jurisdictions agree to send data to GEDTS as part of the GED licensing agreement.		
Natural Resources	1. Staff members who traveled outside Canada on business may have had the ability to access personal information via remote email, Blackberry, personal computer or by other means. 2. Staff members who traveled outside Canada on pleasure may have had the ability to access personal information carried on email or stored in GroupWise via remote access to GroupWise	1. Remote access to GroupWise is protected by username/password authentication and is delivered over an SSL-encrypted link via the secure Blackberry GroupWise server. 2. Remote access to GroupWise is protected by username/password authentication and is delivered over an SSL-encrypted link.	1. When staff travel for business reasons, they are expected to monitor their email and voice mail for business continuity and operational purposes. 2. When staff travel for pleasure, there may be times when they are required or it is desirable for them to maintain contact for operational purposes.

Department	A (Description)	B (Conditions)	C (Reasons)
	email system. 3. Offsite record storage was contracted with Iron Mountain Canada Corporation (subsidiary of the American company). 4. There was no storage of personal information in the custody or control of the Department of Natural Resources outside of Canada during the period. 5. Webex was used for web conferencing.	3. Iron Mountain is to 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 compliance with all applicable privacy legislation.	3. Offsite storage of backup media/microfilm is required as part of the Disaster Recovery Program. The offsite storage is required to ensure vital records can be recovered should an incident occur.
Nova Scotia Business Inc.	1. **salesforce.com inc - CRM data services - storage and access - individuals' business contact information** Pursuant to s. 5(2), the head of Nova Scotia Business Inc (NSBI) determined the storage/ access outside Canada of individuals' business contact	1. **salesforce.com inc - CRM data services - storage and access - business contact information** The individuals' 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	1. **salesforce.com inc - CRM data services - storage and access - business contact information** 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

Department	A (Description)	B (Conditions)	C (Reasons)
	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 principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.	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 compliant.	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.
	2. **VerticalResponse, Inc. - Email campaign management services - individuals' business contact information (primarily email addresses)** Pursuant to s. 5(2), the head of Nova Scotia Business Inc (NSBI) determined the storage / access outside Canada of individuals' business contact information (primarily e-mail addresses) in NSBI's custody / control, as part of e-mail campaign management services supplied under contract by VerticalResponse, Inc. (a US	2. **VerticalResponse, Inc. - Email campaign management services - individuals' business contact information (primarily e-mail addresses)** The individuals' business contact information (primarily e-mail addresses) is to be protected in accordance with the VerticalResponse, Inc. terms of service, privacy statement and anti-spam policy which recognize NSBI as owner of the stored data, provide strong privacy protection and security processes and is US CAN-SPAM Act compliant.	2. **VerticalResponse, Inc. - Email campaign management services - individuals' business contact information (primarily e-mail addresses)** NSBI requires a secure anti-spam compliant e-mail campaign management service that can be integrated with its Salesforce.com CRM service for conducting notification to all or segments of its contacts about events, activities, services of interest to those persons. Domestic suppliers currently do not meet NSBI's technical, service, security and anti-spam requirements.

Department	A (Description)	B (Conditions)	C (Reasons)
	corporation with its principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.		
	3. **International In-market consultants - trade development & investment attraction services - storage and access - personal information (primarily business contact information)** Pursuant to s. 5(2), the head of NSBI determined the storage / access 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.	3. **International In-market consultants - trade development & investment attraction services - storage and access - personal information (primarily business contact information)** The personal information (primarily business contact information) is to be protected in accordance with the service agreement including confidentiality provisions.	3. **International In-market consultants - trade development & investment attraction services - storage and access - personal information (primarily business contact information)** NSBI engages international in-market consultants as an essential and integral 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.
	4. NSBI directors, officers,	**4. NSBI directors, officers, employees - performance of duties during**	**4. NSBI directors, officers, employees - performance of duties during**

Department	A (Description)	B (Conditions)	C (Reasons)
	employees - performance of duties during international travel - storage and access - personal information Pursuant to s. 5(2), 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.	**international travel - storage and access - personal information** 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, Oath of Office and the NSBI Privacy Policy.	**international travel - storage and access - personal information** 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.
Nova Scotia Liquor Corporation	The NSLC did not make any decisions that resulted in the storage of personal information outside of Nova Scotia in 2011. In prior years, we had made decisions that resulted in the storage of personal information outside of Nova Scotia which continue to this day. These have been reported in the year they occurred.	N/A	N/A

Department	A (Description)	B (Conditions)	C (Reasons)
Office of Immigration	While in Europe on business, three staff of the Office of Immigration accessed personal information in emails via IPads or laptop as part of regular operations.	Authorization for traveling across international borders with these electronic devices was authorized by the Deputy Minister in all cases in keeping with government policy and protocol.	
Public Prosecution Service	1. Chief Crown was to be absent in the USA for 18 days .The Blackberry was password protected and was necessary to check for work related messages. 2. There was no storage of personal information outside Canada by the Public Prosecution Service. There was access to personal information using wireless data devices, including BlackBerrys and laptops, on a daily basis while staff were visiting outside of Canada. The locations of the access were: Florida, Mexico, Hawaii, Maine and Massachusetts.	1. Blackberry must be password protected and kept in custody of person during all times. 2. The conditions placed on such access involved the use of encryption and password protection.	1. Messages received were responded to and staff given directions as requested. Information was received from head office and responded to in a timely manner. 2. Such access was granted in order to permit those staff to discharge some of their responsibilities while absent from their offices.

Department	A (Description)	B (Conditions)	C (Reasons)
Securities Commission	One staff member traveled out of country (France) from October 28 - November 14, 2011, for pleasure. The member is soley responsible for all compliance and SRO oversight related work and received permission to take her Blackberry with her. Much of her work is time sensitive, and it is essential she be able to respond to any incoming correspondence which is urgent in nature.	Staff complied with the recommendations provided by the Chief Information Office regarding safe and secure transport and storage of portable storage devices. The device is password protected. Remote access to GroupWise is protected by username/password authentication and is delivered over a SSL encrypted link via the secure Blackberry GroupWise server.	When staff travel outside the country for business or pleasure, they are expected to monitor their e-mail and voicemail where possible to deal with urgent ongoing matters. Therefore, it is necessary for them to check e-mails remotely, where possible, in order to fulfill their responsibilities.
	One staff member travelled out of country (California, USA), for pleasure. She received permission to take her Blackberry out of country to allow her to maintain contact with staff to deal with matters of urgent issues, etc. while away.	Staff complied with the recommendations provided by the Chief Information Office regarding safe and secure transport and storage of portable storage devices. The device is password protected. Remote access to GroupWise is protected by username/password authentication and is delivered over a SSL encrypted link via the secure Blackberry GroupWise server.	When staff travel outside the country for business, training or pleasure, they are expected to monitor their e-mail and voicemail where possible to deal with urgent ongoing matters. Therefore, it is necessary for them to check e-mails remotely, where possible, in order to fulfill their responsibilities.
	November 21 - 23, 2011, one staff member travelled out of country (Baltimore, Maryland,	Staff complied with the recommendations provided by the Chief Information Office regarding safe and secure transport and storage of portable storage devices. The device is password	When staff travel outside the country for business, training or personal reasons, they are expected to monitor their e-mail and

Department	A (Description)	B (Conditions)	C (Reasons)
	USA) for business/committee meeting with the North American Securities Administrators Association. She received permission to take her Blackberry to allow her to maintain contact with staff to deal with matters of urgent issues, etc., while away. December 2 - 10, 2011, one staff member travelled out of country (Ireland) for personal reasons. She received permission to take her Blackberry out of country to allow her to maintain contact with staff to deal with matters of urgent issues, etc., while away. December 3 - 8, 2011, one staff member travelled out of country (Alabama, USA) for training with the North American Securities administrators Association. She received permission to take her Blackberry out of country to allow her to maintain contact with staff to deal with matters of	protected. Remote access to GroupWise is protected by username/password authentication and is delivered over a SSL encrypted link via the secure Blackberry GroupWise server. Staff complied with the recommendations provided by the Chief Information Office regarding safe and secure transport and storage of portable storage devices. The device is password protected. Remote access to GroupWise is protected by username/password authentication and is delivered over a SSL encrypted link via the Blackberry GroupWise server. Staff complied with the recommendations provided by the Chief Information Office regarding safe and secure transport and storage of portable storage devices. The device is password protected. Remote access to GroupWise is protected by username/password authentication and is delivered over a SSL encrypted link via the secure Blackberry GroupWise server. Staff complied with the recommendations provided by the Chief Information Office regarding safe and	voicemail, where possible, to deal with urgent ongoing matters. Therefore, it is necessary for them to check e-mails remotely, where possible, in order to fulfill their responsibilities. When staff travel outside the country for business, training or personal reasons, they are expected to monitor their e-mail and voicemail, where possible, to deal with urgent ongoing matters. Therefore, it is necessary for them to check e-mails remotely, where possible, in order to fulfill their responsibilities. When staff travel outside the country for business, training or personal reasons, they are expected to monitor their e-mail and voicemail, where possible, to deal with urgent ongoing matters. Therefore, it is necessary for them to check e-mails remotely, where possible, in order to fulfill their responsibilities.

Department	A (Description)	B (Conditions)	C (Reasons)
	urgent issues, etc., while away. The Director, Enforcement received permission to take his Blackberry and Laptop out of country (Florida, USA), for pleasure, December 8 - 30, 2011. This allowed him to maintain contact with staff to deal with matters of urgent issues while away.	secure transport and storage of portable storage devices. The devices are password protected. Remote access to GroupWise is protected by username/password authentication and is delivered over a SSLencrypted link via the secure Blackberry GroupWise server.	When staff travel outside the country for business, training, conferences or pleasure, they are expected to monitor their e-mail and voicemail, where possible, to deal with urgent ongoing matters. Therefore, it is necessary for them to check e-mails remotely, where possible, in order to fulfill their responsibilities.
Seniors	No personal information was stored outside of Canada for any project or initiative of the Department of Seniors.	N/A	N/A
Service Nova Scotia and Municipal Relations	1. Twenty-six staff traveled outside Canada during the report period on thirty-nine separate occasions and accessed GroupWise email from a laptop or Blackberry while away. 2. The Interprovincial Record Exchange Program is a system that allows Canadian motor vehicle jurisdictions to securely	1. Remote access to GroupWise is protected by Username/Password authentication and is delivered over an SSL-encrypted link. 2. 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 and AAMVA). Queries are pre-formatted and specific as to what information is displayed. CCMTA has	1. Maintain contact with operations. 2. 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 and infractions occurring in another jurisdiction are recorded on the driver's record in Nova Scotia.

Department	A (Description)	B (Conditions)	C (Reasons)
	query other jurisdiction's driver and vehicle records. The Canadian Council of Motor Transport Administrators (CCMTA) acts as a clearing house and administrators for this system and operates the secure network over which it runs. A partnership arrangement currently exists with the American Association of Motor Vehicle Administrators (AAMVA) to extend the system to the US. 3. Credit card transaction information resulting from payments for on-line services through ACOL or SMSMR, in-person services at Access Centre, Land Registration Offices and the Business Registration Unit, or mail-in services is subject to trans-border data flow through US-based credit information that is transmitted through or stored in the US is at risk of a foreign demand for disclosure under the Patriot Act.	contracts with each of its member jurisdictions that conform to the jurisdiction's privacy legislation concerning disclosure and consent. 3. All service providers in the credit card payment chain are subject to strict security precautions to protect credit card information from unauthorized or accidental disclosure. The service providers are Payment Card industry – Data Security Standards (PCI-DSS) certified and must also follow terms and conditions as defined by the card issuing institutions. Cardholders have agreed to the card issuing institutions' privacy statements that include a notice that third-party service providers may be used to process credit card transactions.	3. SMSMR offers credit card payments as a convenience for customers and to provide efficient and effective on-line services to clients. 4. Access by L-1 Identity Solutions personnel in Billerica and Fort Wayne is an operational requirement in response to

Department	A (Description)	B (Conditions)	C (Reasons)
	4. In 2006, L-1 Identity Solutions (formerly Digimarc) of Billerica, Massachusetts, was awarded a contract to provide Photo License/Photo ID equipment, software integrations and support services to the Registry of Motor Vehicles. This contract included a major upgrade to the Photo License/ID Card system in 2010. The Photo License image/database server (a key component of the system which stores client photos, digitized signatures, personal information and Driver Master Number) is located at the Provincial Data Centre in Halifax, Nova Scotia. In 2006, Digimarc support technicians in Billerica, Massachusetts and Fort Wayne, Indiana were provided remote access via VPN to the image/database server in order to provide tier II/III support. Routine maintenance and support for this system is provided by Halifax-based L-1 field technicians, with the Billerica and Fort Wayne	4. Access from the Billerica and Fort Wayne locations is restricted via VPN username/password and on the image/database server by the privileged account username/password. Access will be in response to escalated support calls only.	Photo License/Photo ID system outages that affect the delivery of customer service.

Department	A (Description)	B (Conditions)	C (Reasons)
	technicians acting as back-up personnel and/or handling escalated problems that the local technicians are unable to resolve.		
Trade Centre Limited	The ticketing system used by Ticket Atlantic is hosted in Irvine, California, USA by Paciolan. The data is housed in their managed facility on their AS6000 mainframe computers. Secure access is provided from TCL facilities to the data centre via a secured VPN tunnel. This is data required for the sale and purchase of event tickets from Ticket Atlantic Box Office and is under the ownership of TLC.	Only Ticket Atlantic employees and agents can access the information through the secured VPN tunnel. Our contract states that Paciolan will only use the collected customer information solely for the purposes contemplated in this agreement and otherwise in compliance with all applicable federal and state laws. (the) Customer will own all personal information, data and related information collected or received through use of the system by it, or directly by Paciolan and all compilations thereof in connection with the operation of the system. Data is stored to ensure we can reconcile delivery of tickets, returns, discrepancies and payment verification to the customer. Customers are asked if they wish to receive future information on events etc. and only then will they be sent any correspondence outside the ticket purchase for which the information was supplied.	In 2004, a tendering process was undertaken to purchase a new ticketing system. Paciolan was chosen as the bid winner as they offer the best solution for requirements. No vendor based in Canada could provide the same level of service necessary. The software vendor only offers a hosted business model – the system is not available to be installed on premises. The contract has been extended for an additional 3 years effective June 1st, 2012. Legal counsel was sought on the original agreement and on the renewal in regard to best practices and privacy requirements and the contract was found to be sound.

Department	A (Description)	B (Conditions)	C (Reasons)
		Others accounts are set up by the customer to purchase tickets online and are maintained for the customer so she/he can purchase tickets online by signing into her/his TA account.	
Transportation and Infrastructure Renewal	Decision made to allow employees' access to GroupWise while outside Canada on business or pleasure was based on the need for staff to maintain contact with the department to deal with urgent matters while away from the office. Access was granted to employees' who requested permission to use their BlackBerry, cell phone and/or laptop to access their e-mails and may have accessed personal information through e-mails via GroupWise. There was no storage of personal information in the custody or under the control of the Department outside of Canada from January 1 to December 21, 2011.	Remote access to e-mails is protected by username/password authentication. All BlackBerries must be password protected and access to GroupWise system was protected by username/password authentication which is delivered over SLL/encryption.	When staff traveled outside of Canada, a travel request form, prepared by staff and management, was approved by the DM prior to travel. Employees who requested permission to use their wireless devices and who may have accessed personal information while outside Canada agreed to comply with the provisions of the Act (Sections 5 & 9). In addition, they agreed to comply with recommendations provided by the Chief Information Office regarding safe, secure transport and storage of portable storage devices. Each year, a memo is sent out to all staff from the DM as a reminder of the legal requirements pertaining to the protection of personal information contained on electronic devices when traveling outside Canada.
Utility and Review Board	Payroll details of Board members and staff were held by Ceridian Canada Inc., a payroll service provider operating in	Records are to be held as confidential by the payroll service provider. Information was stored on servers located in Canada.	Ceridian is a longstanding payroll provider for the Board. A Canadian service provider was sought but none

Department	A (Description)	B (Conditions)	C (Reasons)
	Canada but owned by a parent company resident in the United States.		were found suitable.
Workers' Compensation Board of NS	1. **Employee Access to Personal Information by Mobile Device (IPhone, IPad, Blackberry)** – 21 instances of employee travel outside of Canada with the ability to access personal information through a secure portal into the WCB's internal network via mobile device. 2. **Employee Access to Personal Information by Mobile Device or Laptop** – 10 instances of employee travel outside of Canada with the ability to access personal information through a secure portal into the WCB's internal network via mobile device. 3. **Employee Access to Personal Information by Remote Access** – 325 individual's personal information (contained in unique claim files) accessed from a remote location	1. **Employee Access to Personal Information by Mobile Device (IPhone, IPad, Blackberry)** – Access to WCB's internal network is protected by username/password authentication and is delivered over a secure portal. Immediate report of theft/loss of device or information. 2. **Employee Access to Personal Information by Mobile Device or Laptop** – Access to WCB's internal network is protected by username/password authentication and is delivered over a secure portal. Immediate report of theft/loss of device or information. 3. **Employee Access to Personal Information by Remote Access** – Access to WCB's internal network is protected by username/password authentication and is delivered over a secure portal. Immediate report of	1. **Employee Access to Personal Information by Mobile Device (IPhone, IPad, Blackberry)** – When staff travel for business purposes, they are expected to monitor their email and voice mail for business continuity and to fulfill their job related responsibilities. 2. **Employee Access to Personal Information by Mobile Device or Laptop** – When staff travel for business purposes, they are expected to monitor their email and voicemail for business continuity and to fulfill their job related responsibilities. 3. **Employee Access to Personal Information by Remote Access** – When staff travel for business purposes, they are expected to monitor their email and voicemail for business continuity and to fulfill their job related responsibilities.

Department	A (Description)	B (Conditions)	C (Reasons)
	outside of Canada (in the US) through a secure portal into the WCB's internal network by remote access. 4. **Medical Consultant Access to Personal Information** – 13 instances of access to personal information (contained in unique claim files) accessed from a remote location outside of Canada in the US).	theft/loss of device or information. 4. **Medical Consultant Access to Personal Information** – Information limited to only necessary medical information required to complete a review and provide medical report. All personally identifying characteristics and assigned identifiers redacted to mitigate any potential identification.	4. **Medical Consultant Access to Personal Information** – Medical consultant specializes in both occupational and environmental medicine providing unique capabilities required in the interest of allowing the WCB to administer the *Workers' Compensation Act, Regulations and Policy*.

Table 2: January 1 – December 31, 2011 Foreign Access and Storage by Health Authorities

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Annapolis Valley Health Authority	1. **Contracts:** AVDHA entered into 48 service contracts. These contracts were reviewed by Department Heads to identify if these contracts allowed/required storage or access to personal information outside of Canada. None of the contracts allowed or required access or storage of personal information outside of Canada.	1. All new or renewed contracts have an inclusion clause (see below) added to contracts requiring vendors to comply with *PIIDPA* Legislation. 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 *Personal Information International Disclosure Protection Act* (*PIIDPA*) and any other 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 under the Awarded Contract.	1. Storage and access of personal information outside Canada is linked to pre-existing programs and /or systems utilized in AVDHA and are deemed necessary in the ongoing operations of these systems and programs.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	2. **Travel:** It is our estimation that 16 AVDHA employees travelled outside of Canada. They may have accessed personal information via laptop, Blackberry or PDA's.	2. Laptops, Blackberry devised and PDA's are password protected. Laptops and removable USB storage devices are encrypted (mandatory). Blackberry devices also have an auto-wipe feature (mandatory).SEND (formerly E-Courier) is used for emailing personal information outside of *nshealth.ca* network. Privacy Impact Assessment/Analysis must be completed for all new systems.	
Capital District Health Authority	1. Certain product vendors are permitted to potentially access personal information outside of Canada where required to maintain information technology systems or equipment needed for the operations of the health authority and the requisite expertise is not available within the health authority. 2. Staff members who travel outside of Canada may have had the ability to access personal information via remote	1. All new and renewed contracts where there is information outside of Canada have inclusion clauses requiring vendor compliance with *PIIDPA*. CDHA's Privacy Policy also applies in these situations. 2. All staff who seek remote access to CDHA computer systems must apply for remote access privileges and	1. Current access to and storage of information outside of Canada is linked to pre-existing programs and/or systems utilized in CDHA that have been deemed necessary for operations. 2. Staff members who are travelling may have to access personal information to meet ongoing patient care responsibilities or to ensure business continuity and maintain contact

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	email, blackberry or personal computer.	their devices are assessed to ensure they have the necessary security controls as per the CDHA Remote Access Policy.	with operations.
Colchester East Hants Health Authority	Approximately three employees travelled outside of Canada and may have accessed personal information via remote e-mail, Blackberry, etc., in keeping with district policy.	Has policies associated with restrictions.	Has policies associated with decisions.
Cumberland Health Authority	Decision was made to provide the following (including but not limited to): -VPN access to Dictaphone System from Florida, US offices for remote vendor application support. - Encrypted (SSL) staff access to CHA web mail system from US locations. - Storage of information on whole disk encrypted DHA owned laptops. -Access to email using Blackberry mobile devices. Decisions regarding storage/access of	Access to information stored on CHA networks and servers is only permitted through encrypted VPN connections. All external email access is encrypted through SSL, VPN (IPSEC) or the Blackberry service. The CHA has adopted a standard of encrypting all information on laptops and media that is released outside the CHA. This includes removable media such as encrypted USB storage devices and CD/DVD's. Blackberry devices have been secured with passwords and	Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized in the Cumberland Health Authority and are deemed necessary in the ongoing operations of these systems and programs. Specific criteria related to reporting on decisions of access and storage of information from outside of Canada will be developed.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	personal information outside of Canada are pending upon future guidance: regulations, policies and procedures.	auto-wipe features. Established a process whereby all business changes that may affect the release, use or access to private information as reviewed regularly by the Privacy and Information Management Committees. Privacy Impact Analysis must be completed on all new systems. Guidelines will be developed related to access and storage of personal information outside of Canada.	
Guysborough/ Antigonish Health Authority	VP of Operations took his Blackberry out of the country in April, 2011. CEO took Blackberry out of the country in March, 2011. VP of Community Health took blackberry out of the country in May, 2011.	N/A N/A N/A	Required as part of employment duties. Required as part of employment duties. IT Director informed of plan to take BB. Required for employment duties.

IWK Health Centre	1. **Business Travel:** IWK's records indicate 60 staff members booked 73 different trips through IWK for work-related travel outside of Canada during 2011. The 73 incidents of international travel do not necessarily mean that personal information was stored or accessed outside Canada. IWK staff members do not usually require access to the personal information in IWK's custody and control when travelling outside Canada for work-related purposes and during travel, laptop computers and other mobile electronic devices (including blackberries, iPhones and cell phones) are primarily used for e-mail so staff members can maintain communication with IWK. Staff would not usually take personal information with them or access personal information with these devices during travel.	1. As indicated, when IWK staff travel outside of Canada for work-related purposes, they tend not to access IWK held personal information during the trip. If required, staff can access IWK information systems via secure remote access connections. Staff are encouraged to log-in through protected remote desktop sessions/terminal services, which connect directly to the staff member's computer at the IWK. Technology often used when travelling, such as laptops and handheld devices, are either equipped with encryption software or are password protected. Both measures protect information accessed with/stored on the equipment from unauthorized access and disclosure. In addition, the following restrictions and conditions have been placed on storage and access of personal information from outside of Canada: - 'Active Directory' software protections have been made to	

		Terminal Servers and Remote Desktop Stations, which allow IWK network administrators to control what users are able to do when remotely accessing the IWK network, including the prevention of copy/paste, remote printing and mapping of serial and printer ports. This has been done so that remote access acts as a 'window' into IWK systems, while preventing information from being removed/taken offsite. - Staff are advised during travel outside of Canada to configure handheld devices so that email is not accessible (if not required). The telephone capabilities of the device can still be used. - IWK blackberries and employee/physician iPhones are mandatorily password protected; password use is enforced. The time-out period in which non-use of the device will trigger the requirement to enter a password is five minutes. If a user fails to enter the correct password within a set number of attempts, the device automatically wipes all of its content. Devices can be	

		wiped of all content remotely as well. Further, standards have been implemented to ensure only iPhone devices that support hardware encryption are allowed to integrate IWK's server. - IWK laptops have been and are being updated with encryption software to safeguard information stored on any lost, stolen or improperly accessed laptops including USB portable memory drives used in the laptops.	
	2. **<u>Non-Canadian vendors</u>:** IWK contracts with some specialized service providers who, in the course of providing their services, store or remotely access personal information in the custody and control of IWK outside of Canada. IWK's IT department facilitates the access, and HITS Nova Scotia installs VPN software on services providers' systems. When dealing with large vendors, Site to Site VPN access can be used. Terms of access are	2. When IWK contracts with service providers where there is potential for storage of or access to personal information outside Canada, wherever practicable, IWK obtains individuals' consents or uses contractual conditions to ensure privacy and confidentiality concerns are addressed (including requiring vendors to agree to secure network access requirements, confidentiality clauses, and other accountability measures intended to safeguard personal information). IWK's Privacy	2. The IWK's decisions to allow storage or access of personal information outside of Canada meet the necessary requirements of IWK's operations in the following ways: The vendors with which IWK contracts and who store or remotely access personal information from outside Canada do so as required to deliver their specialized services. Often these vendors are the only companies able to service or maintain the products IWK requires and uses

	contractually controlled. Laboratory testing: IWK contracts with laboratories outside Canada for the provision of certain specialized testing services, which are either not offered in Canada or if they are offered in Canada, the cost is prohibitive. Referral labs in the USA are sought first and if the required testing is not available or appropriate there, European or Australian labs are secured. During the 2011 fiscal year, IWK contracted with 67 laboratories in the USA, 14 laboratories in Europe/UK, and 1 laboratory in Australia.	Office oversees standard remote access given to vendors, and requires vendors to complete remote access forms to limit and control the type of access. And, as part of retaining such services, a 'Privacy Impact Assessment' (PIA) is completed for any new service at IWK which involves the access or storage of personal information outside of Canada. The PIA is reviewed by the IWK Privacy Officer to ensure that risks of disclosure of personal information are properly addressed and mitigated. An example of a non-Canadian service provider is 'Survey Monkey', a web-based surveying tool used by IWK. Because the server for 'Survey Monkey' is located outside of Canada, and therefore so is the data, access to this tool is restricted on IWK's network. The restricted access was implemented and the reasons for it communicated to IWK employees and physicians on May 1, 2009. Access remains restricted to-date, and authorization from the head of	in its day to day operations including specialized software and equipment. Examples of key IWK service providers who may store or access personal information outside of Canada include: - Meditech: Boston, Massachusetts, USA (IWK patient information system) - Agfa: Wilmington, Massachusetts, USA (medical imaging equipment and supplies) - Pyxis: San Diego, California, USA (medical safety systems and technology) - EMC Corporation: Hopkinton, Massachusetts, USA (healthcare data and information sharing services and technology) - Blackbaud: Charleston, South Carolina, USA (non-profit management/accounting software) - Genial Genetics: United Kingdom (laboratory software for genetic data management) - Innovian: Germany and USA (IWK anaesthesia system) IWK sends samples to laboratories outside of Canada for specialized testing services if the cost of having

		IWK is required to access this tool on the network. Laboratory Testing: With respect to laboratory tests conducted outside of Canada, consent is obtained from patients wherever practicable, and IWK Laboratory Services carefully tracks all external laboratory referrals, whether inside and outside of Canada. Further, external laboratories are required to meet certain international standards (e.g. Annex C of ISO 15189:2003) with respect to the collection of information, collection of primary samples, and storage and retention of medical records. IWK's Department of Pathology and Laboratory Medicine has a Laboratory Standards Coordinator, who is responsible for annually monitoring referral laboratories for current accreditation and licensing/certification status under the Department's Evaluation, Selection and Monitoring of Referral Laboratories Policy.	the same specialized testing done in Canada is prohibitive, or if the specialized testing is not available in Canada. Obtaining these specialized laboratory testing services is a necessary requirement of IWK's operations as a health centre, in part because the IWK provides genetic testing for the Maritime Provinces. Genetic testing is an evolving field continually requiring increasingly esoteric testing.
Pictou County	1. Access and storage from outside	1. Vendors are required to	1. Access and storage from outside

Health Authority	Canada is linked to pre-existing programmes and/or systems utilized at PCHA which continue to be required to be used for the necessity in ongoing operation of these systems and programmes (e.g., Meditech, Dictaphone, 3M). 2. PCHA Senior Leaders may have accessed personal information while conducting business outside the country using remote email and Blackberry.	follow PIIDPA legislation. Staff is required to follow PCHA's privacy policies.	Canada is linked to pre-existing programmes and/or systems utilized at PCHA which are required for ongoing operations of these systems and programmes.
South Shore Health Authority	N/A	N/A	N/A
South West Health Authority	1. Seven employees were involved in thirteen international trips where they maintained access to the organization through cell, blackberries, remotely through VPN or through the nshealth.ca web network. The countries involved are the USA (Chicago, New York, New Hampshire, Vermont and Maine), Cuba, Dominican Republic and Mexico. All staff members reported that they maintained daily contact for organizational reasons. 2. In 2011, South West Health Authority entered into service	1. A one hour access to SKYPE for Physician recruitment. 2. The district continues to add the inclusion clause regarding the management of information	2. SWH uses software vendors located outside Canada who maintain

	agreements for the following vendors/instruments/models: - Lab •Radiometer/ABL5(QGH);/ABL8 25; •Somagen Diagnostics/Tissue-TekVIP 5 Bench •Siemens/Clinitek Atlas (SSH) •Bio-Rad Laboratories Evolis Twin Plus •Fisher Scientific/Tissue embedding centre •Biomerieux Inc./Vitek2-60/Bact/Alert 120 Blood Culture System D-120-combination/Variant Analyser 2702600 - Respiratory • Cardinal Health Canada (source) Cardinal Health Inc. Respiratory equipment - Diagnostic Imaging • GE Healthcare/logique e BT09	in all requests for proposals, new contracts, warranties or renewals.	system remotely, for example, Meditech (Health Information), SAP (financial and personnel); Nuance (transcription/dictation), Siemens (DI equipment). Again, the access to systems are managed by written agreements and monitored by SWH. Specialized lab testing either unavailable in Canada or cost prohibitively in Canada are sent outside the country.

	Ultrasound • Agfa Inc./IMPAX CS5000 - Health Information • Nuance/transcription services - Operating Room • Alcon Canada Inc./Eyelift laser In 2011, South West Health Authority entered into Warranty agreements with the following vendors: - EKG • GE Healthcare/MAC5500 ECG System - Diagnostic Imaging • GE Healthcare Ultrasound Voluson E8 Expert BT10		

Table 3[2]: January 1 - December 31, 2011 Foreign Access and Storage by Universities

Universities	A (Description)	B (Conditions)	C (Reasons)
Cape Breton University	1. **Alumni/Donor Database:** CBU uses software provided by an American vendor, Blackbaud, located in South Carolina. Although the system originates from the US, data on university alumni and donors is housed on servers at the CBU campus. Blackbaud does provide remote technical service. If authorized by the university, it is possible for a Blackbaud technician to access. 2. **Student Information System:** CBU Faculty may access portion of the CBU Student Information System when out of the country for the purposes of viewing the records of students in their respective courses and entering term grades. This could be the result of a faculty being out of the country during the period	1. **Alumni/Donor Database:** Access is restricted to authorized technical support carried out by working with a CBU employee possibly on-line. Access to this information is authorized for the purpose of required assigned duties and research. 2. **Student Information System:** Access to student records is restricted to those employees in positions requiring access to fulfill their job responsibilities at the university and is managed through authorized user accounts. Student access is limited to viewing their own recorded	1. **Alumni/Donor Database:** The system is required to meet the operational requirements of the university. The need for remote access from Blackbaud is minimal (1-2 times annually). 2. **Student Information System:** The system is required to meet the operational requirements of the university.

[2] Acadia University, Nova Scotia Agricultural College, Atlantic School of Theology and University of King's College reported that they had no foreign access or retention of personal information outside of Canada.

Universities	A (Description)	B (Conditions)	C (Reasons)
	of time grades are submitted or by a faculty teaching a distance program. Students have web access to the student information system to view their individual financial and academic records.	information and is managed through authorized student accounts.	
	3. **Course Management System:** CBU uses MOODLE as its course management system. The system facilitates on-line learning for both on-campus students and those studying from a distance. Web access is available to this system for both faculty delivering courses and students enrolled in the courses.	3. **MOODLE:** Access to MOODLE is restricted to those faculty delivering and students registered in CBU courses during a particular term. The data accessed is restricted to course materials.	3. **MOODLE:** The system is required to meet the operational requirements of the university.
	4. **Travel:** Approximately 40 staff members have traveled outside of Canada with web access to their personal email via smart phone, tablet or laptop. While travelling outside the country, such access is necessary for university administrators, researchers and other employees to perform their	4. **Travel:** Web access to travelling employees is restricted to email and is available to authentication users only.	4. **Travel:** Remote access to email is required by employees to meet the operational requirements of their positions.

Universities	A (Description)	B (Conditions)	C (Reasons)
	assigned duties or as a necessary part of a research project.		
Dalhousie University	1. **Financial Services:** Service provider for the creation of templates for various electronic financial services, e.g. purchase orders, bills, cheques, etc. 2. **University ID Card:** Management of access and financial processes used through the University ID Card.	1. **Financial Services:** Limited access: only where required for maintenance and troubleshooting. Personal information stored internally. 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. 2. **University ID Card:** Limited access: only where required for maintenance and troubleshooting. Contractual security measures: all personal information will be stored in Canada; 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	1. **Financial Services:** This is the only product offered which offers integration with the University's well-established on-line information systems, which is essential to the function of our Financial Services and Human Resources departments. This service provider has been used since 2003 and offers a significant price advantage to the suite of various products offered by Canadian vendors which would have to be purchased in order to achieve the same degree of program integration. 2. **University ID Card:** This system is proprietary in nature and is only sold and supported by this company. The University's identification card is used by all staff, faculty and students for a variety of purposes, including access to facilities, financial transactions on and off campus, and various administrative functions. Proper management of this integrated tool is necessary for the administrative functions of the University.

Universities	A (Description)	B (Conditions)	C (Reasons)
		time restrictions, audit function, and pre-approved IP addresses; removal of personal information prior to return of hardware, where possible. The company has a support technician located in Canada who provides support whenever possible.	
	3. **Employment Tool:** Comprehensive online tool to assist students in seeking employment.	3. **Employment Tool:** Limited access: only where required for maintenance and troubleshooting. Contractual security measures: all personal information will be stored in Canada; 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.	3. **Employment Tool:** Providing tools for students to develop job-seeking skills is an important and necessary element of the University's student services program. This product was identified as superior in this aspect and no similar Canadian product was identified which provides the necessary functionality and range of services.
	4. **Network and Systems Upgrade:** Consulting services related to the University's ongoing upgrade of its internal network and systems.	4. **Network and Systems Upgrade:** Limited access - only where required for maintenance and troubleshooting. Contractual security measures: restrictions on access to and	4. **Network and Systems Upgrade:** Consultant services, provided by the current provider of the systems, are being upgraded and thus has the expertise to provide the services required. These systems are necessary for the operation of

Universities	A (Description)	B (Conditions)	C (Reasons)
		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.	integral Dalhousie computing services.
	5. **Wireless Products:** Service provider for wireless products for employees, long distance and teleconferencing services.	5. **Wireless Products:** Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees. Internal security measures: process in place to minimize disclosure of personal information.	5. **Wireless Products:** Mobile communications solution for employees, as well as long distance calling and teleconferencing, are essential for administrative operations of the University. Significant price advantage with this service provider through the MASH sector rates negotiated by the Province.
	6. **Warranty Maintenance:** Product warranty maintenance for electronics (Storage in United States).	6. **Warranty Maintenance:** 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 service provider for maintenance or replacement. In many cases, the customer has already provided their personal information to	6. **Warranty Maintenance:** 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.

Universities	A (Description)	B (Conditions)	C (Reasons)
		service provider for warranty purposes. Customers are informed at time of collection that the information they provide will be sent to service provider outside of Canada.	
	7. **Maintenance support** for product which allows University staff and faculty to schedule and manage meetings and activities in an integrated environment.(Remote access for maintenance from United States).	7. **Maintenance Support:** 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.	7. **Maintenance Support:** The ability to effectively schedule and manage meetings and activities is necessary for Dalhousie operations. This product offers superior functionality and range of service not identified in any Canadian alternatives; access rarely required.
	8. **Maintenance support** for academic product used extensively by faculty for online teaching. (Remote access from US).	8. **Maintenance Support 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.	8. **Maintenance Support:** The provision of online teaching opportunities 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 cost to convert; access rarely required.
	9. **Maintenance support** for	9. **Maintenance Support**	

Universities	A (Description)	B (Conditions)	C (Reasons)
	statistical software product, used in course teaching and research (Remote access from US).	**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. Access to personal information for maintenance purposes will rarely, if ever, be required: research using this product will rarely ever contain personal information, and dummy data can be created to illustrate a problem for maintenance purposes.	9. **Maintenance Support:** Necessary for Dalhousie academic and research operations in several departments. This product offers superior functionality and range of service, according to evaluations conducted by users; access rarely required.
	10. **Academic Software:** supports teaching activities and allows for online collaboration, e.g. voice, video, application sharing, etc. (Information stored on server located in Canada, however access from the US may still be required for maintenance purposes). The product is a set of applications used for collaboration in teaching, which are fully	10. **Academic Software:** The company agreed to move storage of our personal information to a server in Canada in 2008. Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees. Personal information is stored on a server located in Canada, hosted by a trusted service provider with	10. **Academic Software:** Necessary for Dalhousie's academic programs in a variety of disciplines; no Canadian product offers a comparable suite of products, service and functionality, combined with integration of other University computing services. Investigations found that this is the only suite of these products on the market, in

Universities	A (Description)	B (Conditions)	C (Reasons)
	integrated with other existing University applications. (Access from the US).	whom we have existing agreements, who are also under obligations of confidentiality. Contractual measures in place to restrict access to and disclosure of information by service provider and their employees.	Canada or elsewhere, that provide access control and integration with our existing applications. These tools are necessary for the operation of the University's academic programs, as student demand for collaborative teaching tools continues to grow.
	11. **Service provider maintenance** for its hardware and software products used extensively throughout the University. Mostly done on-site, however in some cases failed equipment which may contain personal information may need to be returned to service provider in the US.	11. **Service Provider Maintenance:** Contractual measures in place to restrict access and disclosure of personal information to service provider and its employees: access to university systems will be subject to Dalhousie protocols including time restrictions, on-site security, and audit function. Where possible, personal information will be removed from products which require service.	11. **Service Provider Maintenance:** Hardware and software from this service provider are used around the clock in University data centres and other operations, e.g. servers, switches, printers, etc. Maintenance coverage is necessary to our ability to maintain 24/7 operational requirements for these products.
	12. **Maintenance support** for a web-based database that manages information and processes related to student work experience placements in industry. (Remote access from US).	12. **Maintenance Support:** 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	12. **Maintenance Support:** Effectively managing information and processes for student work placements is necessary for the operation of Dalhousie co-operative education programs, particularly in

Universities	A (Description)	B (Conditions)	C (Reasons)
		time restrictions, audit function, and pre-approved IP addresses.	Architecture, Commerce, Computer Science, and Engineering. Cost prohibitive for Canadian alternative; access rarely required.
	13. **Maintenance support** for product which allows for real-time synchronization of faculty and staff calendars with wireless tools. (Remote access from US).	13. **Maintenance Support:** 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.	13. **Maintenance Support:** Making calendars available on the wireless tools used by the faculty and staff who are required to use them is necessary for Dalhousie operations. There is no suitable Canadian alternative, given Dalhousie IT architecture and costs to convert; access rarely required.
	14. **Plagiarism Detection:** Academic program: online plagiarism detection service (Storage in US).	14. **Plagiarism Detection:** 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.	14. **Plagiarism Detection:** 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.
	15. **Maintenance support** for product which supports all major University administrative	15. **Maintenance Support:** Contractual security measures: restrictions on access to and	15. **Maintenance Support:** Necessary

Universities	A (Description)	B (Conditions)	C (Reasons)
	computing applications.(Remote access from US or Bangalore, India)	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.	service for the operation of integral Dalhousie academic computing services; no Canadian alternative identified; access rarely required.
	16. **Maintenance support** for facilities management product used for reserving rooms on campus, specifically for event and classroom scheduling. (Remote access from US).	16. **Maintenance Support:** 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.	16. **Maintenance Support:** The ability to effectively manage room bookings across campus through one centralized program is necessary for Dalhousie operations. This product offers superior functionality to the identified Canadian alternative, and there would be a heavy cost to convert in terms of labor and acquisition costs. Access rarely required.
	17. **Maintenance support** for academic product which provides students with information regarding their progress towards meeting their degree requirements (Remote access from US).	17. **Maintenance Support:** 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.	17. **Maintenance Support:** 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.
	18. **Maintenance support** for	18. **Maintenance Support:**	

Universities	A (Description)	B (Conditions)	C (Reasons)
	a scheduling and data tracking software, designed for university student advising and counseling (Remote access from US).	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.	18. **Maintenance Support:** 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.
	19. **Maintenance Support:** 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 US). 20. **Evaluations:** Software product used to collect and maintain evaluations specifically in the medical education field (e.g. student evaluations, preceptor evaluations, etc.). This product was originally developed in	19. **Maintenance Support:** 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. 20. **Evaluations:** Data is stored internally. 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	19. **Maintenance Support:** 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 alternatives identified; access rarely required. 20. **Evaluations:** Medical education evaluations are a necessary requirement of the operation of our Faculty of Medicine; proper management of these evaluations is critical to decision-making with respect to promotion throughout a student's medical education. This tool was

Universities	A (Description)	B (Conditions)	C (Reasons)
	Canada, however is now a wholly-owned subsidiary of a US company. Product is still maintained in Canada.	function, pre-approved IP addresses, and segregation of personal information where possible. Vendor agrees that any remote access will only occur from within Canada.	originally investigated and purchased when it was 100% Canadian-owned and operated, and a determination was made at that time that it was the most effective tool for our purposes.
	21. **Academic Software:** Service provider licenses to the University certain content in the form of digital books and provides software and technology services to make the content available to its students, faculty and administration in the field of dentistry (licensor located in US).	21. **Academic Software:** Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees.	21. **Academic Software:** Product superior in terms of service and functionality including a complete digital library of dental content from all major publishers, in offline, online and mobile modalities.
	22. **Hardware/Software:** Lease and maintenance multifunction devices (copy/print/scan/fax devices) (vendor headquartered in Japan).	22. **Hardware/Software:** Contractual security measures: restricted access to hard drive during maintenance; removed at end of lease; confidentiality agreement; internal technical controls to limit access to information network segregation; encrypted communication; limited	22. **Hardware/Software:** No Canadian alternatives identified. Awarded through a tender process.

Universities	A (Description)	B (Conditions)	C (Reasons)
		outbound destinations; prohibited inbound connections; internal administrative controls to limited access to personal information.	
	23. **Website Feedback:** Online software enabling visitors to give feedback on the web pages. Feedback not tied to identifiable individual unless visitor opts to provide email address. Licensor located in Israel.	23. **Website Feedback:** Restricted access through server authentication and data encryption and no IP logging.	23. **Website Feedback:** Superior functionality: a strategic component of an interactive website that is in constant touch with customers, and helps identify problems and patterns quickly. No Canadian alternatives identified.
	24. **Plagiarism Detection:** Academic program: online plagiarism detection service (Storage in US).	24. **Plagiarism Detection:** Technical security measures: data security controls in place; Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; Internal security measures: process in place to minimize disclosure of personal information.	24. **Plagiarism Detection:** 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. Data security controls in place. Minimal personal information disclosed.
	25. **Clinical Experience Software:** Software for tracking anonymous student	25. **Clinical Experience Software:** Technical security measures: data security controls in place; Contractual security	25**. Clinical Experience Software:**

Universities	A (Description)	B (Conditions)	C (Reasons)
	clinical experiences and feedback. 26. **Student Engagement Survey:** Student survey about academic experience of law school students. 27. **Crowd Sourcing Product:** Online tool to post questions and answers relating to information technology services.	measures: restrictions on access to and disclosure of information by service provider and their employees; Internal security measures: process in place to minimize disclosure of personal information. 26. **Student Engagement Survey:** Technical security measures: data security controls in place; Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; Internal security measures: process in place to minimize disclosure of personal information. 27. **Crowd Sourcing Product: Technical Security Measures** - hosted in a secure server environment that uses firewall, encryption; Internal security measures: restricted access, minimal disclosure of personal information. 28. **Campus Recreation**	Necessary to monitor effectiveness and improve student clinical experiences in an electronic format for efficiency and accuracy. There is currently no product in Canada offering a comparable range of service and functionality. Data security controls in place. Minimal personal information disclosed. 26**. Student Engagement Survey:** Necessary to assess the quality of service delivered to law students and compare to other Canadian law schools. There is currently no comparable product offered in Canada. Data security controls in place. Minimal personal information disclosed. 27. **Crowd Sourcing Product:** Improves efficiency in asking and responding to questions and overall IT services provided to students and staff. There is currently no product in Canada offering a comparable range of service and functionality. Data security controls in place. Minimal personal information disclosed.

Universities	A (Description)	B (Conditions)	C (Reasons)
	28. **Campus Recreation Impact Study:** Student survey to measure student recreational experiences.	**Impact Study:** Technical security measures: data security controls in place; Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; Internal security measures: process in place to minimize disclosure of personal information.	28. **Campus Recreation Impact Study:** Necessary to assess the quality of recreational services delivered to students and compare to other Canadian schools. There is currently no comparable product offered in Canada. Data security controls in place. Minimal personal information disclosed.
	29. **Hosted Learning Management System:** Academic product used extensively by faculty for online teaching.	29. **Hosted Learning Management System:** Technical security measures: data security controls in place; Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; Internal security measures: process in place to minimize disclosure of personal information.	29. **Hosted Learning Management System:** The provision of online teaching opportunities 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 cost to convert. Data security controls in place. Minimal personal information disclosed.
	30. **Maintenance Support for Student Learning Outcomes Software:** Academic product used by Faculty of Engineering	30. **Maintenance Support for Student Learning Outcomes Software:** Technical security measures: restrictions on access to and disclosure of information	30. **Maintenance Support for Student Learning Outcomes Software:** Relates to larger effort at curriculum mapping and assessment with engineering and pending changes to accreditation process. There is

Universities	A (Description)	B (Conditions)	C (Reasons)
	to plan, implement and measure student learning outcomes supporting curriculum objectives and graduate attributes. 31. **Maintenance Support for Environmental Health & Safety Database:** Software system to track and monitor environmental health & safety incidents. 32. **Maintenance Support for Online Exams:** Software to administer online law school exams.	by service provider and employees; remote access to university systems is subject to Dalhousie protocols. 31. **Maintenance Support for Environmental Health & Safety Database:** Technical security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems is subject to Dalhousie protocols. 32. **Maintenance Support for Online Exams:** Technical security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems is subject to Dalhousie protocols.	currently no comparable product offered in Canada. Access controls in place. 31. **Maintenance Support for Environmental Health & Safety Database:** Software system necessary to adequately track and monitor incidents, superior functionality and support than competitors. Access controls in place. 32. **Maintenance Support for online Exams:** Specialized software used exclusively in law schools in Canada, United States and United Kingdom. There is currently no comparable product offered in Canada. Access controls in place.
Mount Saint Vincent University	Storage outside Canada: We did not store any information such as employee data, student records, or information outside Canada. Access from Outside	There was no limit on the amount of information that a student, faculty or staff member could access from outside Canada within their access	Access to information (from outside Canada) is necessary for students to complete their course work and for faculty and staff to complete their work assignments and/or research. Decisions

Universities	A (Description)	B (Conditions)	C (Reasons)
	Canada: Students, faculty and staff (whether travelling or living) outside Canada were granted to access to email accounts and information systems stored on servers within Mount Saint Vincent University (and within Canada) via email or remote access systems.	rights. The information they have access to is maintained on a server controlled by Mount Saint Vincent University (within Canada).	to allow students to access their course material and relevant data are maintained within the Distance Learning and Continuing Education department and the course/instructor level. Faculty and staff remote access to Mount servers and systems are the responsibility of the department chairpersons or department managers with consultation from Information and Technology and Services. Storage of personal information or data is not currently housed outside of Canada, however any decisions on future hosting of personal information such as Student Email, would need the approval by the Senior Executive Team including the President of the University. As the University must maintain full control of all its data, at all times, any system that the University would consider, in the future, to host information outside of Canada would need to provide significant reduction in costs, administration or increased functionality while providing, at minimum, the same security controls and procedures to protect the University's data.
Nova Scotia College of Art and Design	No storage or access permitted outside Canada during 2011.	Access to personal information from outside Canada is limited to escalated support calls where	Access to personal information from outside Canada is permitted only in situations where alternatives are not

Universities	A (Description)	B (Conditions)	C (Reasons)
		only trained vendor technologists are capable of performing the required tasks and occur only with the expressed permission of the Director of Computer Services.	available or the risk of not allowing access is so great as to jeopardize the normal operation of the institution or the integrity of the data stored.
Nova Scotia Community College	1. The NS Community College has allowed for the storage of personal information under our control to be held by Hobsons EMT (formerly Apply Yourself, Inc.). This company is located in Fairfax, Virginia, U.S. Hobsons EMT is an application service provider offering web-based data management for the College's on-line application process. The College has been using the services of Hobsons EMT effective March 21, 2005, prior to the Assent of the Act on July 14, 2006. 2. In 2011, the College implemented a Blackbaud Inc. fund raising software solution, 'The Raiser's Edge'. Blackbaud Inc. is headquartered in Charleston, South Carolina in	1. The College will provide disclosure to electronic applicants indicating that Hobsons EMT is an American company and the access and use of applications is subject to all applicable federal, state and local laws. 2. Access was provided in a secure manner and was specifically limited to The Raiser's Edge installation. No data was sent outside of Canada.	1.Since our last submission (March 24, 2011), we investigated service providers within Canada, however, there were no emerging or known Canadian companies identified by us through the usual channels conferences, trade shows and vendor contacts. The College continues to seek on-line application solutions through products and functionality available with our current database service provider (Oracle/PeopleSoft) and products. In the meantime, the services of Hobsons EMT are required to support the application process for many of our student applicants.

Universities	A (Description)	B (Conditions)	C (Reasons)
	the United States. The Raiser's Edge installation for the College is locally hosted and maintained in Halifax, NS. However, consultants located in Charleston were accessing information while assisting with the system setup and data conversion. 3. The College will allow employees to transport personal information temporarily outside Canada. We anticipate that this information will be transported using cellular telephones, wireless handhelds, laptops and storage devices.	Access to the system was rescinded upon completion of the Blackbaud Inc. 3. Employees will be required to take all reasonable precautions (e.g. encryption) to protect the personal information.	3. The transport of personal information will be allowed only to the extent that it is strictly necessary for their assigned duties or as a necessary part of a research project. For accessing personal information in College data repositories from outside Canada, the College will permit its employees and students 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.
St. Francis Xavier	1) The University's financial software "Bi-Tech" is provided by a U.S. software vendor Sungard Bi-Tech since 1988. The software requires periodic	1) The University has taken steps to minimize our exposure by restricting access to our system to designated and pre-scheduled time periods and only	1) The cost of switching our software vendors is cost prohibitive at this time.

Universities	A (Description)	B (Conditions)	C (Reasons)
	maintenance and updates. These maintenance needs and updates are applied to our financial software through remote access link between our "Bitech" server located in Chico, California. The access to our server is for software maintenance only. It is theoretically possible that personal information could be accessed at those times – hence this notification.	when maintenance and update activities cannot be accomplished by university personnel. We are working with mature software product and, historically, access has been for semi-annual updates only, therefore, we have minimal exposure points.	
	2) Kinetics software (Kx) is a comprehensive software programme that manages catering, facility and residential bookings. It is comparable to large conference or hotel management systems. The Conferences and Special Events Department at the university uses the programme as our main software to support our operations, making use of the Events, Catering, Marketing and Extracts modules available within the software.	2) Vendor provides technical support through remote access previously arranged with the university technology support group for each incident.	2) The only method of receiving technical support is through remote access by the vendor.
		3) Vendor provides technical support through remote means	3) The only method of receiving technical support is through remote access by the

Universities	A (Description)	B (Conditions)	C (Reasons)
	3) Blackboard Transaction Management system. The system stores names, student ID numbers and meal plan details. Storage is on server in Canada onsite. Remote access is only permitted when a technical issue arises that cannot be resolved. 4) After a review of available systems, a decision was made to purchase a web-based application called EZ Facility to help manage the day-to-day business of Campus Recreation. The application allows for improved membership management, point of sale, scheduling, financial and facility reporting, invoicing and intramural sport organization. Hosting an application on our own servers was not a viable option at time of purchase (and is still not).	previously arranged with the university's technology support group for each incident. 4) The following data is stored in the system: member name, date of birth, address, membership type, membership start and end date, purchases made, time and date of facility entry. Credit cards are not stored in the system and no banking transactions are completed within the system. Anyone we set up with a user account has access to data based on role and permission settings. The following people have full access to data in the system: Campus Recreation Manager and Membership Services Supervisor. The following people have limited access to data in the system: Fitness and	vendor. 4) Data for our EZ Facility account is stored and managed within the Rackspace Data Centres in their Chicago, IL data center. Both Rackspace and EZFacility are PCI Level 1 certified (highest possible) which is Payment Card Industries global standard for data security. This involves tracking and permission limits to accessing account data and personal information.

Universities	A (Description)	B (Conditions)	C (Reasons)
	5) Due to web support and maintenance expertise that could not be performed in-house, the decision was made to have our website (StFX.ca) hosted by a US based company called Acquia in the fall of 2011. This company was selected due to their expertise with the content management software that StFX.ca was built upon.	Wellness Supervisor, Intramural and Facility Coordinator and Clerk. In addition, clerks who work the check-in desk have limited access to membership information for purposes of receiving members and processing purchases. 5) Collected information is stored on Acquia.com servers for a period of time until StFX employees download and delete the information. As such, that personal information may be stored in Acquia.com backup storage systems for a period of time as well. StFX employees log in to the Acquia.com servers and so StFX.ca user names and passwords pass through the Acquia.com servers. However, those user names and passwords are stored and managed within servers located at StFX not on Acquia.com servers.	5) As mentioned, the technical expertise to host and support StFX.ca was found with the company. Acquia has unique expertise dealing with StFX.ca/s content management system – expertise that is not found in Canada.
St. Mary's University	1. **Software Update:** Management software for all aspects of our residence operation from room	1. **Software Update:** All information is stored on a secure dedicated server at SMU. Restricted remote access	1. **Software Update:** To refresh the operating software to a newer version.

Universities	A (Description)	B (Conditions)	C (Reasons)
	assignments, to student billing, to summer conference operations, to incident management. 2. **Plagiarism Detection:** Academic program: online plagiarism detection service (Storage in US) 3. **Maintenance Management System:** The software is a Maintenance Management System that acts as the requesting system for indentified key users on campus and the issuing and tracking of work request and preventive maintenance work for all building on campus. 4. **Travel:** Members of the University travelling outside the country have access to their personal email via smart phone	granted to update under the supervision of in-house technical staff. 2. **Plagiarism Detection:** Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees. Internal security measures: process in place to minimize disclosure of personal information. 3. **Maintenance Management System:** The system holds the names of the buildings and room numbers for all building and history of all maintenance activities. The system has the e-mail addresses of all management, office and maintenance staff in Facilities Management and approximately 20 key users on campus. 4. **Travel:** Employees will be required to take all reasonable precautions (e.g. encryption) to protect personal information.	2. **Plagiarism Detection:** Necessary for Saint Mary's University'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 is disclosed. 3. **Maintenance Management System:** This system is required to meet the operational requirements of the university. 4. **Travel:** Remote access to email is required by employees to meet the operational requirements of their

Universities	A (Description)	B (Conditions)	C (Reasons)
	or laptop. 5. **Facilities Asset Management System:** The software system that tracks the campus buildings and infrastructure and provides a 30 year plan on the renewal of all parts of the buildings and infrastructure. It contains information on the size and condition of all building structures and their systems.	5. **Facilities Asset Management System:** Limited access to 10 Facilities Management office staff and thus hold their email address.	positions. 5. **Facilities Asset Management System:** This software is a common system used by all Atlantic Canada universities and most universities across Canada.
Université Sainte-Anne	Université Sainte-Anne entered into a contractual agreement with a company named Blackbaud. This company provides software to the Université to manage its student information system. Blackbaud also provides hosting services for the database that is created using their software. The database is housed in Boston, Mass.	Access is limited to the Université as a user, Blackbaud as the service provider.	The hosting service is not available in Canada by the service provider. Legal counsel was obtained to ensure the Université was permitted to enter such an arrangement prior to giving consent.

Table 4[3]: January 1 - December 31, 2011 Foreign Access and Storage by School Boards

School Boards	A (Decision)	B (Conditions)	C (Reasons)
Annapolis Valley Regional School Board	1. One individual residing in the U.S. (Tallahassee, FL) had access to a server owned by AVRSB and housed in Canada. The server stored 'Educator's Handbook/Student Discipline Referral' software and related student data. The individual with access was the author of the software. This software is no longer in use and the server was shut down in June, 2011. The individual in the U.S. no longer has access to AVRSB servers or data. 2. AVRSB is one of seven Nova Scotia school boards using the Aesop system for the scheduling and placement of substitute teachers in schools. Frontline Technologies Canada is the contracted service provider of this system. Software and data used in this system reside in Toronto, Canada. The system is supported and maintained by FTC's parent company, Frontline Placement Technologies (FPT), which is located	1. While in use, access was permitted only when necessary for maintenance or upgrading of software. 2. The Department of Education and seven school boards have signed a contract with FTC that clearly states information will be kept private and confidential and will not be released to any third party unless authorized by the DOE and school board in writing. Several conditions exist to ensure data protection: - Frontline has read and agreed to provisions of PIIDPA legislation. The contract also contains provisions for protection of personal information.	1. This software was necessary for day-to-day work of teachers and for monitoring purposes, in order to track and report student discipline issues. It was considered the best option at reasonable cost to perform these functions, until discontinued in June, 2011. 2. This system was selected by school boards because the software is superior to other products on the market and meets the needs of school boards. The vendor was able to satisfy DOE concerns regarding protection of information by agreeing to contractual requirements related to Nova Scotia

[3] Tri-County Regional School Board, Conseil scolaire acadien provincial and Atlantic Provinces Special Education Authority did not store or have access to personal information outside of Canada.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	in the U.S. (Philadelphia, PA). FPT requires periodic access to the data in order to provide technical and end user support and to perform system maintenance. FPT was chosen as the successful bidder in response to a Request for Proposal that was awarded by the Department of Education in October, 2007.	- FTC contracts data centre services with SunGard Availability Services for housing school board data and the Aesop system at their Toronto, Canada location. Data access by FPT is restricted and provided only on an as-needed basis in response to school board requests for support or for system maintenance. Access must be logged and reported to DOE monthly, and must only be for the period of time necessary to complete work. Access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. - The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. - All equipment used for Aesop implementation in Nova Scotia is owned by FTC, and is stored at SunGard in locked wired cages. Access is restricted to FTC personnel. - Employees of FPT have signed confidentiality agreements with the company. - Only personnel authorized by the school board will be provided access to the board's electronic information. - The data contained in the system is limited to that required for operations. It includes	privacy legislation as well has housing the data and system in Canada.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
		employee name, professional number, home address, phone number, email address, skills/qualifications, work schedule availability, sick leave entitlements, records of absenteeism, teaching assignments completed and hours worked.	
Cape Breton-Victoria Regional School Board	1. The Cape Breton-Victoria Regional School Board required an improvement to the process of placing substitute teachers in schools. This function was taking a substantial amount of administration time to organize skill profiles, determine which substitutes could be used for the selected vacancy and contact substitutes manually by phone to fill absences. As a result, the School Board has contracted the services of Frontline Technologies Canada Inc. (FTC) for the scheduling and placement of substitute teachers in schools in response to filling teacher absences. Other participating school boards are: Annapolis Valley, Halifax, Chignecto-Central, South Shore, Strait Regional and Tri-County. The Aesop System provided by FTC is an automated tool used for	1. The Department of Education and 7 School Boards have signed a 5 year contract with FTC that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by DOE and the School Board in writing. The following conditions exist to ensure Nova Scotia's data is protected: a. Frontline has read and agreed to the provisions of the PIIDPA legislation. The contract also has extensive provisions for protection of personal information including the requirement for FTC to notify DOE if they receive a foreign order or request to disclose personal information, i.e., an order pursuant to the *Patriot Act* or similar legislation). b. FTC has contracted data centre services with SunGard Availability Services (SunGard) for housing Nova Scotia's data and the Aesop system infrastructure at their Toronto location. The School Board data is housed at the SunGard data centre and system support services are provided	1. The DOE, on behalf of the school boards, issued an RFP for a software solution that would automate the process of filling teacher absences. The school boards evaluated three proposals and selected the Aesop product because of its superior software functionality and FPT's significant experience in successfully supporting a large user base in other jurisdictions. There was also some experience using this software at one of the school boards. It was found to be a very good product and the vendor support services were excellent. In addition, FTC committed to housing

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	tracking, processing and storing information related to teacher absences. FTC utilizes an application service provider (ASP) model for provision of the system to the School Board. The software and data reside in Toronto and the company is paid a yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) System. The system is supported and maintained by FTC's parent company FPT located in Philadelphia, USA. There are two types of support – technical and end user. Technical support is required to ensure the system is operating as expected and available to the user community and includes such things as performance management, data backup and recovery and software upgrades. End user support is needed to assist the School Board with specific system problems being experienced, answer questions regarding software functionality and provide training information and	by FPT located in Philadelphia, USA. Data access by FPT is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and support. c). The following conditions apply when FPT accesses the School Board data: • The accesses must be logged and reported to DOE monthly; • Access is only for the period of time required to address the issue/problem, and; • Access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The audits are quite detailed and provide clients with an added level of confidence that SunGard are doing the right things to ensure continuance of service and protection of information. The audits encompass all areas of the organization including administration and organization, facilities, logical access, network security, computer operations, backup and recovery processes and change management processes. SunGard has provided the DOE with a copy of the most recent SAS70 Audit. In addition, the facility is ISO 9001:2000 certified by Lloyd's	Nova Scotia's data and the Aesop System in Canada to satisfy the DOE concerns with information security and privacy legislation. The DOE and school boards negotiated and signed a contract with FTC in May, 2008. The system began implementation through Nova Scotia in September, 2008. In summary, this solution was chosen because the software is superior to other products on the market and meets the needs of the School Board. The vendor was able to satisfy the DOE concerns regarding protection of information by agreeing to contractual requirements related to Nova Scotia's privacy legislation as well as housing the data and system in Canada. SunGard is a highly reputable and capable

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	materials related to new system features. FPT requires periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support. FPT were chosen as the successful bidder in response to a Request for proposal (RFP) that was awarded by the Department of Education (DOE) in October, 2007. Effective 2011/2012 school year, this AESOP system was expanded in the Cape Breton-Victoria Regional School Board to include the teacher assistant classification. 2. Approximately 8 staff members travelled outside Canada and may	Registry Quality Assurance. d). All equipment used for the Nova Scotia Aesop implementation is owned by FTC. The equipment is stored at SunGard in individual locked wire cages and access is restricted to FTC personnel. In addition, SunGard is compliant with industry standards and best practices for data centres including privacy of data, separate network segments, remote control cameras, raised flooring, fire detection and suppression systems, cooling, water sensors, electronic monitoring and uninterruptible power supply systems. e). Employees of FPT has signed confidentiality agreements with the company. f). Only personnel authorized by the School Board will be provided access to the School Board's electronic information. g). The data contained in the system is limited to that required to ensure successful operation. It includes employee name, professional number, home address, phone number, email address, skill profile including qualifications, work schedule availability, sick leave entitlements, records of absenteeism, teaching assignments completed and hours worked.	organization and were very cooperative in allowing the DOE to conduct an on-site audit of their facility and processes. FTC have signed off on all security and information privacy clauses in the contract, understand and agree to comply with the province's PIIDPA legislation, do not store data in the US, and use secure methods for all data transmissions. Also, all data accesses by employees of the parent company (FPT) are restricted to specific purposes and logged and reported to DOE monthly. 2. Functionality of the operations of the board are

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	have, or had the ability to, access personal information via remote email, blackberry and/or personal computer.	2. All personnel information is housed on-site with existing infrastructure. All blackberries and personal computers are password protected.	deemed necessary for management and operations. The staff members at issue occupy management positions and must be available by email.
Chignecto-Central Regional School Board	1. The Chignecto-Central Regional School Board (School Board) required an improvement to the process of placing substitute teachers in schools. This function was taking a substantial amount of administration time to organize skill profiles, determine which substitutes could be used for the selected vacancy, and contact substitutes manually by phone to fill the absences. As a result, the School Board has contracted the services of Frontline Technologies Canada Inc. (FTC) for the scheduling and placement of substitute teachers in schools, in response to filling teacher absences. Other participating school boards are: the Annapolis Valley Regional School Board, Cape Breton-Victoria Regional School Board, Chignecto-	1. The Department of Education and seven school boards have signed a five year contract with FTC that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by DOE and the School Board in writing. The following conditions exist to ensure Nova Scotia's data is protected. Frontline has read and agreed to the provisions of the Personal Information International Disclosure Protection Act (PIIDPA) legislation. The contract also has extensive provisions for protection of personnel information, including the requirement for FTC to notify DOE if they receive a foreign order or request to disclose personal information (i.e. an order pursuant to the Patriot Act or similar legislation). Frontline Technologies Canada Inc. has contracted data centre services with SunGard Availability Services (SunGard) for housing	1. The DOE on behalf of the school boards issued an RFP for a software solution that would automate the process of filling teacher absences. The school boards evaluated three proposals and selected the Aesop product because of its' superior software functionality and FPT's significant experience in successfully supporting a large user base in other jurisdictions. There was also some experience using this software at one of the school boards, it was found to be a very good product and the vendor support services were excellent. In

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	Central Regional School Board, South Shore Regional School Board, Strait Regional School Board, and Tri-County Regional School Board. The Aesop System provided by FTC is an automated tool used for tracking, processing, and storing information related to teacher absences. Frontline Technologies Canada Inc. utilizes an application service provider (ASP) model for provision of the system to the School Board. The software and data reside in Toronto, Canada and the company is paid a yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. The system is supported and maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA. There are two types of support, technical and end user. Technical support is required to ensure the system is operating as	Nova Scotia's data and the Aesop system infrastructure at their Toronto, Canada location. The School Board data is housed at the SunGard data centre and system support services are provided by FPT located in Philadelphia, USA. Data access by FPT is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and support. The following conditions apply when FPT accesses the School Board data i) the accesses must be logged and reported to DOE monthly ii) access is only for the period of time required to address the issue/problem, and iii) access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The audits are quite detailed and provide clients with an added level of confidence that SunGard are doing the rights things to ensure continuance of service and protection of information. The audits encompass all areas of the organization including, administration and organization, facilities, logical access, network security, computer operations, backup and recovery processes, and change management processes.	addition, FTC committed to housing Nova Scotia's data and the Aesop System in Canada to satisfy the DOE concerns with information security and privacy legislation. The DOE and school boards negotiated and signed a contract with FTC in May of 2008. The system began implementation throughout Nova Scotia in September 2008. In summary, this solution was chosen because the software is superior to other products on the market and meets the needs of the School Board. The vendor was able to satisfy the DOE concerns regarding protection of information by agreeing to contractual requirements related to Nova Scotia privacy legislation, as well as housing the data and system in Canada.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	expected and available to the user community, and includes such things as performance management, data backup and recovery, and software upgrades. End user support is needed to assist the School Board with specific system problems being experienced, answer questions regarding software functionality, and provide training information and materials related to new system features. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support. Frontline Placement Technologies were chosen as the successful bidder in response to a Request for Proposal (RFP) that was awarded by the Department of Education (DOE) in October 2007.	SunGard has provided the DOE with a copy of the most recent SAS70 Audit. In addition, the facility is ISO 9001:2000 certified by Lloyd's Registry Quality Assurance. All equipment used for the Nova Scotia Aesop implementation is owned by FTC. The equipment is stored at SunGard in individual locked wire cages, and access is restricted to FTC personnel. In addition, SunGard is compliant with industry standards and best practices for data centres; including, privacy of data, separate network segments, remote control cameras, raised flooring, fire detection and suppression systems, cooling, water sensors, electronic monitoring, and uninterruptible power supply systems. Employees of FPT have signed confidentiality agreements with the company. Only personnel authorized by the School Board will be provided access to the School Board's electronic information. The data contained in the system is limited to that required to ensure successful operation. It includes: employee name, professional number, home address, phone number, email address, skill profile including qualifications, work schedule availability, sick leave entitlements,	SunGard is a highly reputable and capable organization and were very cooperative in allowing the DOE to conduct an on-site audit of their facility and processes. FTC have signed off on all security and information privacy clauses in the contract, understand and agree to comply with the province's PIIDPA legislation, do not store data in the US, and use secure methods for all data transmissions. Also all data accesses by employees of the parent company (Frontline Placement Technologies) are restricted to specific purposes and logged and reported to DOE monthly.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
		records of absenteeism, teaching assignments completed, and hours worked. An on-site audit of the SunGard data centre facility was conducted by DOE on August 27, 2008, to confirm the vendor's ability to protect school board's personal information.	
	2. A number of Chignecto-Central Regional School Board employees traveled outside of Canada and had the ability to access personal information contained in email or stored in the GroupWise email system, using devices such as the Blackberry, laptops, tablets and iPads.	2. Remote access to GroupWise is protected by surname/password authentication and is delivered over an SSL-encrypted link via the secure GroupWise server.	2. When staff travel for business reasons, they are expected to monitor their email and voice mail where possible. It is necessary for them to check email remotely.
	3. The Provincial Student Information System (SIS) is used by the Nova Scotia education systems to manage school operations, including processes such as student registration and enrolment, attendance, student scheduling, etc.	3. The DOE has implemented security measures to protect electronic storage of personal information and other information in SIS. It is maintained in a secure environment house in Halifax, N.S. The contract with the service provider stipulates that the DOE staff authorize access to the environment by Pearson technical staff located in Rancho Cordova, California, USA for the purpose of providing periodic technical support.	3. The decision to contract with Pearson for provision of the Student Information System was reached after an extensive evaluation of vendor products through a tendering process. Pearson was chosen due to its superior functional capability in meeting the requirements of the Nova Scotia education system as well as its standing as a

School Boards	A (Decision)	B (Conditions)	C (Reasons)
			leading distributor of the SIS software worldwide.
Halifax Regional School Board	Fifteen staff members travelled outside of Canada which would have had access to personal information via their Blackberries, IPhones or laptop computers.	Relevant HRSB policies would apply to Blackberry, IPhone and computer is password protected. The HRSB will incorporate into its policy direction on access and storage of personal information outside of Canada.	Staff members at issue occupy management positions and must be available by email for decision making and information purposes.
South Shore Regional School Board	1. Travel: use of laptops and blackberries outside of Canada. A number of SSRSB employees accessed their web mail, or used their phones in the following countries: USA, Dominican Republic, Mexico, and Cuba. 2. Tech Support: AESOP (absence reporting), Grouplink (helpdesk software), Easy Bus (transportation management), In-School (student information system), Zimbra (web-based email), Kaspersky (anti-virus), HP server support (hardware support), Untangle (anti-SPAM appliance), Taleo (web-based application for employment/hiring),	1. If deemed necessary for employees role, laptops and blackberry usage is allowed outside of Canada. All laptops are password protected; data roaming is turned off on blackberries when possible. 2. For all the noted hardware/software, data is stored in Canada (most often, stored on-site); however, tech support is based in the USA. Occasional remote access is required. Sometimes, as part the troubleshooting process, tech support outside Canada will connect via a remote desktop session. For such sessions, a one-time use password or session id is provided. Once the remote desktop session was ended/closed outside tech support can no longer	1. When deemed to be necessary for employee's role. Most often, staff members at issue are in management roles and their availability is necessary for information purposes and decision-making. 2. All hardware/software is deemed necessary for the daily operations of the SSRSB.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	and PHD virtual back-up software (application support).	access our systems.	
Strait Regional School Board	1. The Strait Regional School Board utilizes the Aesop System provided by Frontline Technologies Canada (FTC) which is an automated tool used for tracking, processing, and storing information related to employee (except janitors and bus drivers) absences. Frontline Technologies Canada Inc. utilizes an application service provider (ASP) model for provision of the system. The software and data reside in Toronto, Canada and the company is paid a yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. The system is supported and maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA. There are two types of support, technical and end user. Technical support is required to ensure the system is operating as expected and available to the user community, and includes such things as performance	1. The Department of Education and the Strait Regional School Board have signed a five year contract with FTC that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by DOE and the School Board in writing. The following conditions exist to ensure the Strait Board's data is protected. Frontline has read and agreed to the provisions of the Personal Information International Disclosure Protection Act (PIIDPA) legislation. The contract also has extensive provisions for protection of personnel information, including the requirement for FTC to notify DOE if they receive a foreign order or request to disclose personal information (i.e. an order pursuant to the Patriot Act or similar legislation). Frontline Technologies Canada Inc. has contracted data centre services with SunGard Availability Services (SunGard) for housing Nova Scotia's data and the Aesop system infrastructure at their Toronto, Canada location. The School Board data is housed at the SunGard data centre and system support services are provided by FPT located in Philadelphia, USA. Data access by FPT is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and	1. Consent to transport Board owned equipment outside of Canada is provided only in instances when it is deemed necessary for management and operations. During 2011, one employee was granted permission to transport a Board owned Blackberry. The employee was travelling for the Nova Scotia International Student Program. The decision was based on the necessity for the employee to contact parents of exchange students in the event of an emergency. The BlackBerry was password/pin protected.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	management, data backup and recovery, and software upgrades. End user support is needed to assist the School Board with specific system problems being experienced, answer questions regarding software functionality, and provide training information and materials related to new system features. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.	support. The following conditions apply when FPT accesses the School Board data: i) the accesses must be logged and reported to DOE monthly ii) access is only for the period of time required to address the issue/problem, and iii) access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The audits are quite detailed and provide clients with an added level of confidence that SunGard are doing the rights things to ensure continuance of service and protection of information. The audits encompass all areas of the organization including, administration and organization, facilities, logical access, network security, computer operations, backup and recovery processes, and change management processes. SunGard has provided the DOE with a copy of the most recent SAS70 Audit. In addition, the facility is ISO 9001:2000 certified by Lloyd's Registry Quality Assurance. All equipment used for the Nova Scotia Aesop implementation is owned by FTC. The equipment is stored at	

School Boards	A (Decision)	B (Conditions)	C (Reasons)
		SunGard in individual locked wire cages, and access is restricted to FTC personnel. In addition, SunGard is compliant with industry standards and best practices for data centres including privacy of data, separate network segments, remote control cameras, raised flooring, fire detection and suppression systems, cooling, water sensors, electronic monitoring, and uninterruptible power supply systems. Employees of FPT have signed confidentiality agreements with the company. Only personnel authorized by the Strait Regional School Board are provided access to the School Board's electronic information. The data contained in the system is limited to that required to ensure successful operation. It includes: employee name, professional number, home address, phone number, email address, skill profile including qualifications, work schedule availability, sick leave entitlements, absenteeism records, teaching assignments completed, and hours worked. An on-site audit of the SunGard data centre facility was conducted by DOE on August 27, 2008, to confirm the vendor's ability to protect school board's personal information.	
	2. The Board currently holds online subscriptions for United streaming and Reading A to Z. These are on		

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	line subscriptions to education media. The teacher's name and school are provided to both on line education media providers. This contract was in existence prior to December 15, 2006. 3. Regarding employees who travel outside of Canada, to our knowledge, twenty seven (45) have accessed/may have (or had the ability to access) accessed personal information via remote email, BlackBerry. The Board has restricted employees who travel outside of Canada with board owned equipment.	3. Employees are required to obtain prior written consent of the head of the Public Body to transport Board owned equipment outside of Canada. Consent to transport Board owned equipment outside of Canada is provided only in instances when it is deemed necessary for management and operations. Employees who utilize Notes Traveler on their iPad, iPod or iPhone are now password protected (also on their own personal devices) to protect personal information. A new security feature has been installed. The SRSB network allows secure VPN access only.	

Table 5 January 1 – December 31, 2011 Foreign Access and Storage by Municipalities[4]

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
Halifax Regional Municipality	1. Sixty nine staff and twenty nine HRP staff travelled outside of Canada and had the ability to access personal information via one or more of the following means: Cell Phone, Blackberry, Laptop, Memory Stick, VPN.	1. Prior to travelling, staff were advised that HRM Communication tools (Cell Phones, Blackberries, Laptops, Memory Sticks, VPN) were to be password protected.	1. The HRM and HRP staff, who travelled outside of Canada with their communication device(s) were expected to maintain a means of communication with their respective staff/Business Unit in order to meet operational responsibilities/requirements.
	2. The following vendors, Versaterm (Police RMS, CAD 911), Hansen (Tax Bill, Customer Service, Permit/License), Open Text (Document Management), Hastus ERP (Metro Transit) RIVA (PSAB Compliance -Financial), SAP (Finance and Crystal Reports), ESRI (GIS), IVOS (Risk Management),	2. Vendor access is controlled and monitored by ICT Support staff.	2. Vendor access is necessary for the systems to continue to function properly.

[4] Nova Scotia Association of Regional Development Authorities, Lunenburg/Queens Regional Development Agency, Cape Breton Regional Municipality; Towns of Annapolis Royal, Bridgewater, Clark's Harbour, Digby, Hantsport, Lockeport, Lunenburg, Mahone Bay, Oxford, Stellarton, Trenton, Truro, New Glasgow, Amherst, Middleton, Mulgrave, Parrsboro, Pictou, Shelburne, Stewiacke, Windsor, Yarmouth; Municipalities of the Districts of Argyle, Barrington, Chester, Guysborough, St. Mary's, West Hants, Yarmouth; and, Municipalities of the Counties of Antigonish, Inverness, Kings, Pictou, Victoria, Municipality of East Hants and Halifax Regional Library Board had no access or storage outside of Canada to report.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	were provided access on an approved, need basis to the applicable production systems for support and maintenance.		
Municipality of the County of Colchester	Ten staff travelled outside Canada. It is known that four staff accessed personal email or stored information and email through GroupWise via a laptop or Blackberry. The employees received permission from senior management.	Employees have been notified to limit email use with Blackberry's and laptops during time out of the country unless absolutely necessary. We have an approved policy that requires employees to limit any personal information being sent while visiting/working outside of Canada, and if they are taking electronic equipment, they are required to report their intention to senior management.	When staff are travelling for business or personal reasons, they may be expected to monitor their business email in order to fulfill their job responsibilities.
Municipality of the District of Lunenburg	1. Two employees travelled outside of Canada and had the ability to access personal information via one or more of the following means: Blackberry, Laptop. During travel in April, one laptop was stolen while going through airport luggage check. Personal drive on laptop may have been exposed.	1. Employees have been advised that the use of municipal equipment that can gain access to personal information is not to be used or taken out of the country without permission. If an employee is required to take electronic equipment outside of the country, prior to travelling, they are to report their intention to the PIIDPA administrator to ensure secure login/passwords and or encryption protocols are in place.	1. Municipality of Lunenburg staff when traveling outside the country maybe expected to monitor their email in order to fulfill operational responsibilities/requirements. Upon notification of laptop be stolen, the laptops active directory account on municipal servers were disabled immediately.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	2. Municipal property owners living outside Canada are sent property tax invoices twice per year (April and September). There are often exchanges in communication via email with these customers.	2. Email activity is controlled and monitored by IT support.	2. This is an operational process that occurs on a regular basis and provides for an efficient manner for customer service.
	3. The following Vendors were provided access on an approved, need basis to the applicable production systems for support and maintenance. (Townesuite/Procom - Taxes/payroll/financial operations, Digitial Fusion - Website Administration, Land Development/HFX Support - Permit tracking system, ADI Ltd - Engineering Services, Atlantic Data Systems Support (Fundy) - Municipal Servers and operating systems, Office Interiors - Photocopiers and printers, Active Network	3. Vendor Access is controlled and monitored by IT Support.	3. Vendor access is necessary in the daily operations of the municipality in order to continue business functions properly.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	Ltd. - Recreation Program Payments system, Select Tech. Corp. - Security Systems, VTSCADA Software - Engineering Services.		
Property Valuation Services Corporation	PVSC has implemented the use of "Time out" – a vacation tracking and scheduling software provided by CWS Software, based in New Jersey, NY, USA. This software is used by PVSC employees for internal use only.	PVSC employees can access their own personal records in Time Out, with the exception of managers, who access the information relevant to the staff they supervise. The only information stored that meets the criteria of "personal" under PIIDPA is the employee names. The contract with CWS contains appropriate confidentiality clauses and provision for destruction of information upon request.	The software is required for appropriate time management and tracking of PVSC employees.