Personal Information International Disclosure Protection Act

2012 Annual Report

NS Information Access and Privacy Office
December 2013

Message from the Minister of Justice

I am pleased to provide the seventh 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 approved "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, 2012 to December 31, 2012 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 63 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: 65 entities reported that there was no access or storage outside of Canada for the 2012 calendar year.

Original signed by

_____

The Honourable Lena Metlege Diab

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, 2012 Foreign Access and Storage by Government Departments, Agencies, Boards & Commissions [1]

Department	A (Description)	B (Conditions)	C (Reasons)
Chief Information Office	1. 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), including Microsoft, Hewlett Packard, IBM, Barracuda Networks, Polycom Inc., Cisco, Dell, Novell, EMC, Checkpoint Software and Tangoe Inc (who bought Symphony Teleca Corporation's Telecom Expense Management System (EMS) business on August 8, 2012).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	1. 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 involve direct access to any personal information. In the rare cases that any access to any personal information might be possible, 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 transferred from Province of Nova Scotia (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	1. 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 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. In the case of Tangoe, Inc., the EMS solution was selected by PNS because Tangoe, Inc. was the best option to ensure PNS telephone billing requirements could be met. Tangoe, Inc.'s prior experience with other PNS telephone billing systems lowered the risk associated with support of the EMS system. There is currently no alternative

[1] Aboriginal Affairs, Agriculture, Fisheries & Aquaculture, Executive Council Office, Nova Scotia Health Research Foundation, Nova Scotia Human Rights Commission, Nova Scotia Legal Aid Commission, Nova Scotia Pension Agency, Nova Scotia Public Service Long Term Disability Plan Trust Fund, Office of Police Complaints Commissioner, Office of Policy and Priorities, Office of the Premier, Advisory Council on the Status of Women, Seniors, Sydney Tar Ponds, Waterfront Development Corporation and Workers' Compensation Appeals Tribunal reported no personal information was accessed or retained outside of Canada.

Department	A (Description)	B (Conditions)	C (Reasons)
	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. In the case of Tangoe Inc., occasional remote access to the EMS application and database in order to perform scheduled support or troubleshooting activities. This access takes place from Tangoe, Inc.'s offices located in Nashville, Tennessee using secure virtual private network software (also running on a server located in the provincial government's data centre).	or problem solving purposes, then it is sent through a secure and encrypted channel. In the case of Tangoe, Inc., a controlled remote access gateway allows the company to view the PNS database used by EMS to store personal information. However, it does not give Tangoe, Inc. the ability to remove or copy any files. Once Tangoe, Inc.'s work is completed, its access to the database is disabled by CIO staff. Under the agreement with PNS, Tangoe, Inc. covenants 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. Tangoe, Inc. 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 Tangoe, Inc. to inspect the security measures it has put in place to protect such personal information.	method of receiving technical support access for EMS within Canada.
	2. CIO employees may have taken mobile devices, such as laptops and blackberries, out of Canada for work purposes in accordance with departmental process and with Deputy Minister approval. These mobile devices are secured with password protection in accordance with security policy.	2. Government-owned mobile devices, such as laptops and blackberries, are only approved for out of Canada travel for work purposes in accordance with departmental process.	2. Staff who are mission critical to sustaining certain services and/or technologies may be approved to take their government-owned mobile device out of the country for support purposes. These mobile devices are secured with password protection in accordance with security policy.

Department	A (Description)	B (Conditions)	C (Reasons)
Communications Nova Scotia	1. Google Analytics (GA) has been recently made the corporate standard for web analytics. Conditions or restrictions that have been placed on storage or access of personal information outside of Canada include: - Internet Protocol (IP) addresses will be 'masked', the last series of numbers in the IP address will be removed before being stored by GA, which reduces the ability to identify specific users' behavior on our websites. - The GA software does not allow government staff access to individual IP addresses. - Access to the analytics information will be controlled by password, and the information will only be presented in an aggregated form. Under the Province's privacy policy, IP addresses are considered personal information. For three Internet-related initiatives, "Nova Scotia Life, Pomegranate, and Canada's University Capital, the CNS Marketing Division, used Google Analytics. 2. Six employees travelled in	1. 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 personal information without prior consent unless it is to comply with applicable laws.) The equipment was accessed only by the Communications Nova Scotia employees.	1. Communications Nova Scotia is accountable in our 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 websites, from where and approximately how long they stayed. This information allows us to refine our marketing and advertising strategies ensuring that we provide best value to the government. 2. The cellphone was needed to make and

Department	A (Description)	B (Conditions)	C (Reasons)
	the United States with a cellphone, BlackBerries and two iPads for business or pleasure. The equipment was used by only them and were password protected except for the cellphone and one iPad.		receive calls. BlackBerries were necessary to make calls and use e-mail. iPads were used to e-mail, post messages on Facebook and access Twitter.
Communities, Culture and Heritage	1. Decision to allow primary service provider (Unisys Canada Inc.) for Internet resource NOVA SCOTIA HISTORICAL VITAL STATISTICS ONLINE (NSHVSO) operated by NS Communities, Culture and Heritage (Archives Division), to outsource to service sub-provider (Skipjack, Cincinnati, Ohio, USA), part of the transaction processing, and storage during processing, of credit card information collected from service clients during online interactive commercial activity.	1. No disclosure to, or retention of credit card personal information by service sub-provider outside Canada except as required to carry out and verify online commercial transactions with NSHVSO service clients.	1. Commercial component of NSHVSO online service depends on client's ability to prepay for copies online via credit card transaction conducted in real time. Due to the global character of today's financial services industry, it is extremely unlikely that online credit-card transactions can be completed and verified without the personal information collected during transaction processing being stored, accessed from or disclosed outside Canada.
	2. Decision to use Google Analytics. Nova Scotia government websites were cleared to use Google Analytics as long as it is in a manner that abides by the methodology outlined in the Privacy Impact	2. In accordance with approved privacy impact assessment noted above.	2. In keeping with Strategic Goal 3 of the Departmental Web Strategy: Provide timely and reliable intelligence that includes regular statistical monitoring and reporting (web analytics).

Department	A (Description)	B (Conditions)	C (Reasons)
	Assessment signed by all Deputy Heads. (2012/08/15) 3. Continued use of Twitter and Facebook accounts. Registered Twitter Accounts include: @NS_Museum, @NS_Archives, @SailBluenoseII, @MNH_Naturalist, @NS_MMA, @FisheriesMuseum, @RossFarmMuseum, @McCullochHouse, @Highlandv, @Sherbrooke_NS, @OfficeofANSARegistered Facebook Accounts include: Nova Scotia Museum, Nova Scotia Archives, MNH Nova Scotia, Maritime Museum, Fisheries Museum of the Atlantic, Ross Farm Museum, Sherbrooke Village, Highland Village, African NS Affairs, Creative Nova Scotia, and Sail Bluenose II with continued use of YouTube Channels. Registered accounts are: Nova Scotia Archives, Nova Scotia Museum, Highland Village Continued use of Pinterest and Pin Map for Nova Scotia Archives.	3. N/A	3. In keeping with Strategic Goal 2 of the Departmental Web Strategy: Create a content rich, well-designed, easy to navigate, relevant and accessible online presence across the department that is user-centered. Social media initiatives will be attached to a clear business driver (communications, outreach, recruitment, program delivery, consultation, employee engagement, workplace collaboration). For the most part, social media initiatives (Web 2.0) will be launched to drive visitors to Web 1.0 sites.

Department	A (Description)	B (Conditions)	C (Reasons)
	4. Decision to launch and maintain a Flickr site, titled 'Nova Scotia Archives Photostream' and registered as http://www.flickr.com/people/nsarchives. Contents on site feature public-domain content uploaded to the site. Link on NSARM Website enables Internet visitors to access the photostream without a Flickr account. Visitors also able to comment on content via phone or e-mail to NS Archives, rather than on Flickr site.	4. N/A	4. In keeping with Strategic Goal 2 of the Departmental Web Strategy: Create a content rich, well-designed, easy to navigate, relevant and accessible online presence across the department that is user-centered. Social media initiatives will be attached to a clear business driver (communications, outreach, recruitment, program delivery, consultation, employee engagement, workplace collaboration). For the most part, social media initiatives (Web 2.0) will be launched to drive visitors to Web 1.0 sites.
	5. 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 of libraries. Without the ILS, libraries could not function. The ILS contains personal information about	5. 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. The contract with SirsiDynix was updated this year to strengthen privacy protection and to codify data access permissions. 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 reasonable and appropriate. SirsiDynix	5. 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)
	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 client's 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.	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.	
Community Services	1. Children In Care of the Minister of Community Services may require treatment services that are not available in the Province of Nova Scotia, and on occasion within Canada. During the 2012 calendar year, five children in care were placed in residential treatment facilities in the U.S. to receive residential treatment services.	1. 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.	1. 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 written

Department	A (Description)	B (Conditions)	C (Reasons)
	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 e-mails with agency social workers in Nova Scotia and paper copies of information identified above.		request by the legal guardian or client, when the client has reached the age of 18 years.
	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	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 NS 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

Department	A (Description)	B (Conditions)	C (Reasons)
	Canadian offices operated in Mississauga, Ontario once issues reported are vetted by Housing Authority IT staff. The data is 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.		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.
Economic and Rural Development and Tourism **A. Information excludes Tourism**	ERDT (excluding Tourism and Procurement and Agencies) does not actively use social media; Communications Nova Scotia manages all posts to social media. A. 1.Approximately 20 staff traveled outside of Canada in 2012 with either a Blackberry or a laptop computer.	A.1. All devices used during travel outside of Canada were password protected and contained the latest security policies installed and managed	A.1. The Blackberries were necessary to make calls and use email. The laptop computers were used to prepare presentations and email.

Department	A (Description)	B (Conditions)	C (Reasons)
	Procurement Website uses Google Analytics as per the direction given by CIO on the usage regarding IP tracking as a government standard for website analytics. A. 2. Procurement twitter account is used to promote public tender listing from the procurement website which includes public sector tender listings. YouTube channel is used to host public webinar recording offered by Procurement Services that appear on the procurement website. A.3. Procurement staff travelled within Canada and used a Blackberry to access email communication or business calls with peers or vendor community.	by the Chief Information Office (CIO). Blackberry devices are password protection following guidelines by CIO. A.2. Procurement twitter account posts public tenders that appear on the website. No personal information is sent publicly or via private messaging. YouTube channel has comments and ratings disabled to limit interaction by users.	A.2. The decision to engage in certain US based social media services was to enhance our outreach activities with the public and vendor community as it relates to the *Public Procurement Act*. A.3. Blackberry smartphones are used for business related activities interacting with the vendor community on-site, trade shows and other functions.
B. Nova Scotia Tourism Agency (ERDT)	B.1. The NS Tourism Agency has an active social media presence including YouTube, Facebook, Twitter, Instagram, flickr and Pinterest. Each of these social media channels stores data outside of Canada. The data captured within these channels are provided by users who voluntarily agree to the	B.1. YouTube, Facebook, Twitter, Instagram, flickr and Pinterest are each username and password protected. Comments on contact used by the NS Tourism Agency are moderated and approved; each social media channel mentioned has its own privacy policy to protect its users.	B.1. The number one influence of travel is referrals from friends and family. Social media channels is the digital space where friends and family actively engage with one another, sharing content in the form of videos, links, photos, referrals, etc. In order to remain competitive in the global market place, destinations must play an active role in social media

Department	A (Description)	B (Conditions)	C (Reasons)
	rules of each social media channel and, thus, have also agreed to the capture of their data and storage of such data outside of Canada.		channels which meet the demographic of the destinations target market. Being active in these channels allows NS to find brand ambassadors, influence positive brand engagement, share relevant content to keep the destination top of mind and ultimately influence travel to the province.
	B.2. The NS Tourism Agency uses Google Analytics to track and measure website statistics. Google Analytics records IP addresses on Google's servers in the US. However, users cannot be specifically identified nor is any personal information given up.	B.2. This information is subject to 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 personal information without prior consent unless it is to comply with applicable laws.	B.2. NS Tourism Agency is responsible for reporting the effectiveness of our website marketing activities. Google Analytics is the best tool in the market to accomplish this task; it is also free. Google Analytics enabled us to collect and report on website statistics such as how many visitors came to our website, from where and approximately how long they stayed and their traffic patterns within the site, etc. This type of knowledge allows us to refine our digital marketing efforts and provide the best value to the government.
	B.3. The NS Tourism Agency uses Mail Chimp to send out promotional email campaigns. The agency uses Mail Chimp because of the high degree of flexibility, features and the very low cost of the service. Mail Chimp is a US company and does have access to our email subscriber list which would	B.3. When users subscribe to the promotion email list, all information submitted is voluntary, protected by the *Freedom of Information and Protection of Privacy Act* and a form is available to users to change and / or remove their personal information from the email list. Mail Chimp's terms of conditions state that they will not, under any circumstances, sell your lists, contact	B.3. Mail Chimp and Constant Contact are used because it allows the NS Tourism Agency a high degree of flexibility in managing email lists, easy to use, cost effective and these external tools can be used in conjunction with external agencies such as the Agency of Record and the Digital Development Agency whom often have issues accessing email systems with the

Department	A (Description)	B (Conditions)	C (Reasons)
	include first name, last name and email address. In addition, when promotional emails are sent using Mail Chimp, personal information such as IP address, browser type and user habits are stored enabling us to track how successful the email campaign was (i.e., open rates, links clicked, etc.).	people on your lists, market to people on your lists, steal your lists or share your lists with any other party unless it is required by law. All information stored in Mail Chimp is username and password protected.	government firewall.
	B.4. The NS Tourism Agency uses Constant Contact to manage the Travel Media contact list. In 2012, the contact list was set up and managed, however, no promotional emails were sent from this account. Constant Contact is a US based company and does have access to our email subscriber list which would include information such as email address.	B.4. Constant Contact privacy policy states that they will not sell, share or rent this information to others in ways different from what is disclosed in their privacy statement which include requirement by law and merger or acquisition.	
	B.5. Approximately 11 staff traveled outside of Canada in 2012 with either a Blackberry, laptop or IPad.	B.5. All devices used during travel outside of Canada were password protected except for one iPad. The iPad was only used for work related communications to access GroupWise for email messages and to post to government social media channels all of which were password protected.	B.5. The Blackberries were necessary to make calls and use email. The laptops and iPads were used to prepare presentations, email, and post messages on social media channels.

Department	A (Description)	B (Conditions)	C (Reasons)
Education	1. **Provincial Student Information System:** 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. Department 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 parent's 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. **Teacher Certification Fee Processing:** The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the US 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. **Teacher Summer Professional Development Registration System:** 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.	3. 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.	3. The option of payment by credit card payments is a convenience for teachers, and provides efficient and effective online services.
	4. **Travel with electronic devices:** A number of Department of Education staff traveled outside Canada for business and/or pleasure, and had the ability to access	4. Remote access to staff email accounts through GroupWise and Microsoft Outlook is protected by username/password authentication and is delivered through a combination of VPN	4. Staff are 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.

Department	A (Description)	B (Conditions)	C (Reasons)
	personal information contained in email or stored in the GroupWise or Microsoft Outlook email system using devices including cell phones, iPads, BlackBerries and laptops. Staff seek permission from the head of the public body before taking devices across the Canadian border.	and encryption.	Laptops and IPads are needed for preparing documents, and accessing email and Internet sites.
	5. **TIENET:** The Extended Services and Programming system is a component of the provincial Student Information System and is used by the Nova Scotia education system (schools, school boards, Department of Education) to manage the student documentation associated with the Program Planning Process such as Individual Program Plans, Documented Adaptations, Health/Emergency Care Plans, Special Transportation Needs and Schools Plus information. The system contains personal information regarding students and parents, including names, addresses, phone numbers, email addresses, medical, program planning and academic records. This information about students and parents is	5. The Department of Education has implemented reasonable security measures to protect electronic storage of personal and other information in the Extended Services and Programming system. 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 (MAXIMUS) stipulates that Department of Education staff will authorize access to the environment by MAXIMUS technical staff located in Eatontown, New Jersey, USA, for the purpose of providing periodic technical support. Staff monitor and audit to ensure the access is reasonable and appropriate. MAXIMUS has no operational requirements to access personal information about clients. Therefore, the risk of access to student and parents' personal information by MAXIMUS is low, but it is technologically possible.	5. The decision to contract with MAXIMUS for provision of the Extended Services and Programming system was reached after an extensive evaluation of vendor products through a public tendering process. MAXIMUS 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 Special Education Case Management software worldwide.

Department	A (Description)	B (Conditions)	C (Reasons)
	necessary for the Nova Scotia education system to manage student program delivery in the areas noted above for students in Grade Primary to 12.		
Energy	Twenty-two staff were permitted to transport personal information devices, such as laptop computers, cell phones, and electronic data storage devices outside Canada or used computers outside of Canada to access their work email accounts 53 times.	Remote access to staff email accounts through web access to Outlook is protected by username/password authentication over an HTTPS secure connection. Staff use of Blackberry devices provides email delivered over an SSL-encrypted link via the secure BlackBerry server. Blackberry devices and laptops are password protected.	Staff are sometimes required to monitor their email and voicemail for business continuity purposes. BlackBerry devices were necessary to make calls and access email. Laptops are required for preparing documents, and accessing email and Internet sites. Staff use of remote web access to government email provides for business continuity.
Environment	An Executive Director was out of country in the past year and had their blackberry with them..	The blackberry was turned OFF while the Executive Director was out of the country.	They used the blackberry to answer work e-mails at the CANADIAN Airports on the way to/from their destination.
Film Development Corporation NS	Approximately three staff members traveled outside Canada on business. These staff members had the ability to access personal information carried on email or stored in GroupWise and Outlook via remote access (Blackberry and laptop) to the GroupWise and Outlook email system.	N/A	When staff are traveling outside of Canada for business reasons, they are expected to monitor their email in order to fulfill their job responsibilities.
Finance	**1. Remote Access via Blackberry:** There were 2 instances that staff members were approved to take their Blackberry while travelling	1. Permission must be granted in order to take a Blackberry out of the Country. Remote access to e-mail is protected by username/password authentication and is delivered over a secure server link (SSL)	1. 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 e-mail via Blackberry.	encrypted link. All Blackberries must be password protected.	
	2. Remote Access: Staff members who traveled outside Canada may have had the ability to access personal information contained in e-mail via remote e-mail by personal computer.	2. 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.	2. When staff travel, they may be required to conduct business or maintain contact with operations.
	3. The Department of Finance operates SAP systems for the public sector including provincial departments, school boards, regional housing authorities, district health authorities and 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	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	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)
	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 and carried out by SAP staff resident in SAP service locations such as the United States, Ireland, Brazil, Germany and India.	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 maintained. There is no storage of data from SAP systems outside Canada.	
	4. Royal Bank of Canada (RBC) was awarded a contract in 2010 by the Province to provide electronic vendor payments to US vendors / individuals for the period 2011 to 2013.	4. 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 effect the transfer of the funds is not endorsed by NACHA and, in some cases, may be illegal. Each bank, in the US, must comply to the rules of NACHA. Vendors opt into receiving electronic payments. They are required to complete an application form, consenting to have payments forwarded	4. 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 flow through an Automated Clearing House. There is no ACH that stores information in Canada.

Department	A (Description)	B (Conditions)	C (Reasons)
		to them via our electronic vendor payment (EVP) system.	
Halifax-Dartmouth Bridge Commission	HHB MACPASS software application maintenance and support is provided by 3M (previously VESystems) primarily located in Irvine, California. 3M provides both routine maintenance and upgrades and have access to personal information through a portal to HHB's internal network. Access is fairly routine and would occur minimally once a month.	3M's access is controlled through a secure virtual private network and the services are provided for under the terms set out in an annual service agreement.	The MACPASS back office software application is a proprietary software application that is critical to Halifax Harbour Bridges 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 since implementation.
Health and Wellness	**1. McKesson Corporation SHARE** - Horizon Provider Portal McKesson Corporation Horizon Provider Portal (HPP) is the viewer used to access the provincial Electronic Health Record or SHARE (Secure Health Access Record) by authorized clinicians throughout the province. The software vendor, McKesson, is providing on-going support and software changes as needed. The McKesson developers may need to access the local provincial system from their US based office to deploy software fixes and to provide support. SHARE	**1. McKesson Corporation – SHARE** - McKesson's development staff will use a pre-existing secure 'data tunnel' to provide support to the multi-component provincial Electronic Health Record or SHARE. SHARE consists of the Horizon Provider Portal, Horizon Clinical Infrastructure, Horizon Clinical Repository and the STAR Patient Processing system. These are located in the HITS-NS data center. All users accessing the data will require security sign-on to SHARE. Select McKesson developers/testers will have access to the provincial Electronic Health System or SHARE. McKesson developers/testers will be pre-approved and must sign a confidentiality agreement. McKesson	**1. McKesson Corporation – SHARE:** The McKesson developers may need to access the local provincial system from their US based office to deploy software fixes and to provide support. The Horizon Provider Portal is the tool used to view the personal health information housed in the Horizon Clinical Repository, as such; personal health information may be viewed during testing and support activities. The viewer component is required when accessing the Horizon Clinical Repository. The Horizon Clinical Infrastructure is an integration environment which houses the Horizon Clinical Repository, as such; personal health information may be viewed during testing and support

Department	A (Description)	B (Conditions)	C (Reasons)
	- Horizon Clinical Infrastructure McKesson Corporation Horizon Clinical Infrastructure (HCI) is the technical foundation used to house the McKesson components of the provincial Electronic Health Record or SHARE (Secure Health Access Record). The software vendor, McKesson, is providing on-going support and software changes as needed. The McKesson developers may need to access the local provincial system from their US based office to deploy software fixes and to provide support. SHARE - Horizon Clinical Repository McKesson Corporation, Horizon Clinical Repository (HCR) is the patient centric repository of health information for Nova Scotians. The repository is the central component of the Electronic Health Record or SHARE (Secure Health Access Record). The software vendor, McKesson, is providing on-going support and software changes as needed. The McKesson developers may need to access the local provincial system from their US based office to deploy software fixes and to provide support STAR	developer's/testers access will be terminated immediately at test completion - test completion was forecast to March 31, 2012. Support access will be on-going. No personal information will be downloaded or copied by McKesson. All requests will be tracked, and audit reports provided as required for review. McKesson Corporation is committed to following all Health Insurance Portability and Accountability Act (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. The McKesson developers may need to access the local provincial system from their US based office to deploy software fixes and to provide support. Personal health information may be viewed during testing and support activities. No personal information will be downloaded during these activities.	activities. The integration component is required to support the Horizon Provider Portal and the Horizon Clinical Repository. The Horizon Clinical Repository was selected after a market /product scan, a gap assessment and was approved through a Ministerial Approval and Alternative Procurement. STAR Patient Processing 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)
	Patient Processing The McKesson Corporation 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 Record's (EHR or SHARE's (Secure Health Record)) integration requirement for patient active admissions, discharges and transfers. The 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 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. **2. FairWarning**: FairWarning is an appliance based	**2. FairWarning:** The Master Agreement with FairWarning prohibits storage or access of personal	**2. FairWarning:** The FairWarning application will be used to augment current user access audit approaches for

Department	A (Description)	B (Conditions)	C (Reasons)
	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 on-going 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 data.	information outside of Canada unless the Department of Health and Wellness 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 center. Select FairWarning project managers/developers/testers will have access to the 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 to following all Health Insurance Portability and Accountability Act (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.	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.
	3. <u>Relay Health:</u> Relay Health has remote access to the	**3. <u>Relay Health:</u>** Relay Health does not	**3. <u>Relay Health:</u>** McKesson Canada's

Department	A (Description)	B (Conditions)	C (Reasons)
	information system for tier three level technical support when enabled by the 811 Operator. Relay Health does not have access to patient data.	have access to patient data. When enabled by the 811 Operator, Relay Health will be granted access to the general information system for tier 3 technical support.	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.
	4. <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 interpreters may be located in any one of a number of countries in or outside North America. Calls involving interpreters are not audio recorded nor do the interpreters document any details of the call; therefore no recorded information is collected or stored outside of Canada.	**4. <u>Language Line Services:</u>** Language Line obtains a signed confidentiality agreement from each respective interpreter and reviews these agreements once annually. The interpreter service is provided over the phone. Language Line Services, as per McKesson Canada'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 throughout the encounter. Access to personal information is granted after obtaining consent from the caller to engage third party interpretation services to facilitate the call in the caller's language of choice. Interpreters do not audio record or document details of the call.	**4. <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 party interpretation service is required to address linguistic barriers. The interpreter service is provided over the phone.
	5. <u>DOH Employee Access:</u> Thirty-two (32) staff of the Department Health and Wellness traveled outside Canada on business and had the	**5. <u>DOH Employee Access:</u>** The Department of Health and Wellness Transmission of Confidential Information by E-mail and Fax guideline	**5. <u>DOH Employee Access:</u>** When staff is traveling for business reasons (e.g. meetings, conferences) they are expected to monitor their e-mail and voice mail where possible. Therefore, it is necessary

Department	A (Description)	B (Conditions)	C (Reasons)
	ability to access personal information carried on e-mail or stored in GroupWise/Outlook via remote access to the GroupWise/Outlook system.	(2004) prohibits the inclusion of personal information in e-mail sent outside the GroupWise/Outlook system unless the e-mail is encrypted and password protected. The Guideline also recommends limiting the inclusion of personal information contained in e-mail within the GroupWise/Outlook system. Therefore, the amount of personal information held or sent by e-mail 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.	for them to check e-mail remotely where possible in order to fulfill their responsibilities.
In*NOVA*Corp	There were 9 employees who travelled for business or pleasure and, of those 9 employees, there were 12 different acts of access which included VPN access, Blackberry access and or webmail access. Most activity occurred within North America but access was also made in Mexico. In addition, Innovacorp uses the following during the normal course of business: IBM Global Services expense management platform Jan 1, 2011-Dec 31, 2012WebEx Jan 1, 2012-Dec 31, 2012 Web conferencing purposes; Surveymonkey Jan 1, 2012-November 30, 2012 Employee	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, In*Nova*Corp 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)
	survey purposes Skype Jan 1, 2012-Dec 31, 2012 Web conferencing purposes FacebookJan 1, 2012-Dec 31, 2012 Social marketing purposes Twitter Jan 1, 2012-Dec 31, 2012 Social Marketing purposes Slimtimer Jan 1, 2012-Dec 31, 2012 On line tracking purposes Deal Flow Jan 1, 2012-December 31, 2012 On-line deal management tool Drop Box Jan 1, 2012- December 31, 2012 On-line file storage tool.		
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/shredding vendor is a subsidiary of a US based company. The information is not transferred outside of Canada. Intergovernmental Affairs has been systematically withdrawing records from Iron Mountain and all records were by February 21, 2013.	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 Intergovernmental Affairs as it utilizes to safeguard its own confidential information.	At the time of the decision, Intergovernmental Affairs had limited space and business activities were creating records that remain relevant for long periods of time. Iron Mountain was specifically chosen because, at the time, no Canadian owned competitor in Nova Scotia was available. Furthermore, they were/are considered to be leaders in their industry for records security. Since 2009, Intergovernmental Affairs has been systematically withdrawing its records from Iron Mountain and transferring them to its central registry, the Provincial Archives and the Government Records Centre as appropriate. Intergovernmental Affairs is pleased to report that as of February 21, 2013 all records have been removed from Iron Mountain.

Department	A (Description)	B (Conditions)	C (Reasons)
Justice	A. **Correctional Services** 1. After reviewing proposals to an RFP, it is clear that there were no qualified companies could offer a system which would store data only in Canada. JEMTEM 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, Canada, Boulder, Colorado, US and Decatur, Georgia, US respectfully.	A. **Correctional Services** 1(a). JEMTECS' Project Manager and the Provincial Electronic Supervision Coordinator are the only persons authorized to establish user accounts (logins and passwords) for the host monitoring system. 1(b). Only JEMTEC Inc. and Department of Justice personnel designated by the NS Department of Justice shall have 'permanent' user access to the host monitoring system. JEMTECS' Project Manager shall immediately notify NS Department of Justice 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. 1(c). 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	A. **Correctional Services** 1. This access is necessary to ensure optimal service and to maintain automated monitoring systems that communicate system issues such as hardware failures, software abnormalities or other operating environment issues that may arise. JEMTEC Inc. and its subcontractors require access to the operating system and software in order to complete regular system maintenance functions required to ensure mission critical operation of the system.

Department	A (Description)	B (Conditions)	C (Reasons)
		provides senior administrators with a tracking tool for quality control and data security purposes. Access to the system is via a standard internet browser with 128 bit SSL encryption, with predefined timeouts to lock out users after periods of inactivity after they have logged in, for security purposes.	
	2. One staff person traveled outside of country with a Blackberry that contained personal information (work related).	2. 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.	2. Permission to take Blackberry out of the country was granted to allow contact with staff and to deal with matters or urgent issues while travelling.
	B. **Serious Incident Response Team** One staff person traveled outside of country with a Blackberry and laptop that contained personal information (work related).	B. **Serious Incident Response Team** 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**. Serious Incident Response Team** Permission to take Blackberry out of the country was granted to allow contact with staff and to deal with matters or urgent issues while travelling. This staff person required to have their Blackberry and laptop with them as they are the only person who can authorize the commencement of an investigation or the laying of charges. They are also responsible for the approval of any media releases.
	C. **Medical Examiner's Office** Five staff persons traveled outside of country and used	C. **Medical Examiner's Office** Employees are expected to maintain communication with staff at the office	C. **Medical Examiner's Office** Permission to take Blackberry out of the country was granted to allow contact with

Department	A (Description)	B (Conditions)	C (Reasons)
	their Blackberries that contained personal information (work related). D. **Emergency Management Office** 1. In 2005, EMO purchased an electronic information management system called eTeam from NC4 Corporation of California, USA that is installed and maintained on provincial government servers within the Provincial Government's Data Center. Support for this electronic information system is provided via an annual maintenance contract by an NC4 technical support person from the US. During the calendar year of 2012, on at least one occasion, but not more than five individual times, the technical support person in the US remotely accessed the eTeam system to implement upgrades to the system. 2. One staff person traveled outside of country with a Blackberry that contained	and ensure that their Blackberries and laptops are password protected and that the Government server (which is encrypted) is utilized. D. **Emergency Management Office** 1. Remote access control to the eTeam system is set up and maintained by the provincial government's Chief Information Office personnel as, and when, required for maintenance to the system. This is initiated each time by provision of a remote access user name and password to the technical support person in the US who remotely accesses the eTeam system to apply patches and updates to the system. 2. Employees are expected to maintain communication with staff at the office and ensure that their Blackberries and	staff and to deal with matters or urgent issues while traveling. D. **Emergency Management Office** 1. Access to the eTeam system by the American technical support person is for the sole purpose of implementing their annual enhancements to the system. 2. Permission to take Blackberry out of the country was granted to allow contact with staff and to deal with matters or

Department	A (Description)	B (Conditions)	C (Reasons)
	personal information (work related).	laptops are password protected and that the Government server (which is encrypted) is utilized.	urgent issues while travelling.
	E. **Legal Services** 1. Automon, Legal Services Pratice Manager (PM) vendor, had access to the server on a few occasions during the period. Tier II application maintenance support to provide routine upgrade through a proxy remote access desktop session. There was no access to personal information at any time. The personal information was password protected and the vendor did not have a password. Staff watched the vendor at all times to ensure no personal information was accessed.		E. **Legal Services** 1. Automon is the only available vendor for PM and the update was necessary for the litigation group to continue functioning.
	2. Five staff persons used their Blackberries outside of Canada. The Blackberries contained personal information (work related).	2. 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.	2. Permission to take Blackberry out of the country was granted to allow contact with staff and to deal with matters or urgent issues while traveling.
	F. **Public Safety and Security** Two staff persons traveled out of country and used their	F. **Public Safety and Security** Employees are expected to maintain	F. **Public Safety and Security** Permission to take Blackberry out of the

Department	A (Description)	B (Conditions)	C (Reasons)
	Blackberries and laptops that contained personal information (work related).	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.	country was granted to allow contact with staff and to deal with matters or urgent issues while traveling.
	G. **Policy and Information Management** 1. In July, 2004, the Department of Justice entered into a service contract with Iron Mountain Canada Corporation to provide 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.	G. **Policy and Information Management** 1. Information held in a confidential and secure manner as outlined in agreement with Iron Mountain.	G. **Policy and Information Management** 1. The Department of Justice entered into this contract as there was insufficient storage available at Records Centre.
	2. Two staff persons used their Blackberries outside of country. The Blackberries contained personal information (work related). outside of Canada	2. 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 utilize	2. Permission to take Blackberry out of the country was granted to allow contact with staff and to deal with matters or urgent issues which traveling.
	H. **Court Services** One staff person traveled outside of country with a Blackberry that contained personal information (work	H. **Court Services** Employees are expected to maintain communication with staff at the office and ensure that their Blackberries and laptops are password protected and that	H. **Court Services** Permission to take Blackberry out of the country was granted to allow contact with staff and to deal with matters or urgent issues while traveling.

Department	A (Description)	B (Conditions)	C (Reasons)
	related). I. **<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 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 Government server (which is encrypted) is utilized. I. **<u>Maintenance Enforcement Program (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.	I. **<u>Maintenance Enforcement Program (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)
	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 submitted to the designated authority by a person who is seeking to enforce, establish or vary a support of maintenance order, where the other party resides outside Nova Scotia. The documents are submitted to the designated authority with a request that same be sent to the reciprocating jurisdiction in which the other party resides. The designated authority is		

Department	A (Description)	B (Conditions)	C (Reasons)
	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.		
Labour and Advanced Education (includes Office of Immigration)	1. There were approximately eleven 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. None of the laptops, which were taken outside of Canada for departmental purposes, contained any personal information.	1. Authorization for traveling across international border with these electronic devices was authorized by the Deputy Minister in all cases in keeping with government policy and protocol.	
	2. The Department of Labour and Advanced Education (LAE) utilizes NRSPro.com software for the purpose of storing and processing information, in support of the General Educational Development (GED®) program.	2. The department has a contract with NRSPro which stipulates that all information will be kept private and confidential and will not be released to any third party unless authorized by the department in writing. The contract also states that only personnel authorized by the department will be provided access	2. The department completed an evaluation of options for delivery of the Nova Scotia GED® program in November of 2001. 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

Department	A (Description)	B (Conditions)	C (Reasons)
	The GED® is composed of a 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 1500 tests conducted each year in Nova Scotia. The department scans the test	to store and retrieve Nova Scotia information.	Canadian requirements. Both vendors were application service providers (ASPs) 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 to conform with GEDTS program changes in 2002. This would have resulted in an interruption in client service to allow time to design the system and obtain certification from 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

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 re-writing 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. The test scoring is completed remotely by NRSPro and the test results and certificates are transmitted to the department in PDF files for printing locally. The transmission is over a SSL connection using an encrypted link. The test results and certificates are also available for viewing by authorized LAE staff on the NRSPro website, using the same security methods. A user ID and password is also required for		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 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)
	access. In addition, 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. This includes gender, age, country, province, number of participants, number/percentage passed, and number/percentage failed. 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. The GED Testing Service (www.GEDtest.org) is a		

Department	A (Description)	B (Conditions)	C (Reasons)
	program of the American Council on Education (ACE) which develops, delivers, and safeguards the GED Test, setting the policy for and ensuring compliance of test administration. GED testing is administered by each of the 50 states and the District of Columbia, the Canadian provinces and territories, the U.S. insular areas, U.S. military and federal correctional institutions. On March 15, 2011, ACE in partnership with Pearson announced the creation of a new business, GED LLC to design, develop and deliver a new GED test. The new GED Testing Service is to be based in Washington, D.C. with additional offices in Minneapolis, Minnesota.		
Natural Resources	There was no storage of personal information in the custody or control of the Department of Natural Resources outside of Canada from January 1, 2012 to December 31, 2012. 1. Staff members who traveled outside Canada on business may have had the ability to access	1. Remote access to email accounts is protected by username / password	1. When staff are travelling for business reasons, they are expected to monitor their email and voice mail for business

Department	A (Description)	B (Conditions)	C (Reasons)
	personal information via remote e-mail, 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 e-mail or stored in GroupWise or Outlook via remote access to GroupWise or Outlook email system. 3. Offsite record storage was contracted with Iron Mountain Canada Corporation (subsidiary of the American Company).	authentication and is delivered over an SSL-encrypted link via the secure Blackberry GroupWise / Outlook server. 2. Remote access to email is protected by username / password authentication and is delivered over an SSL-encrypted link. 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 arrangements in compliance with all applicable privacy legislation.	continuity and operational purposes. 2. When staff are traveling for pleasure, there may be times when they are required, or it is desirable for them, to maintain contact for operational purposes. 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) PIIDPA the head of Nova Scotia Business Inc (NSBI) determined the storage / access outside Canada of individuals' business contact information in NSBI's custody / control, as part of customer	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 stored data and provide strong privacy protection and security processes. The service is certified as a 'Safe Harbour'	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 through independent evaluation and based on its superior standing in meeting

Department	A (Description)	B (Conditions)	C (Reasons)
	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.	under the EU Directive on Data Privacy and is certified 'TRUSTe' privacy compliant.	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. - E-mail campaign management services - individuals' business contact information (primarily e-mail addresses)** Pursuant to s. 5(2) PIIDPA, 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 corporation with its principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.	2. **VerticalResponse, Inc. - E-mail 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. - E-mail 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.
	3. **TinderBox.com inc. - Sales proposal management service**	3. **TinderBox.com inc. - " Sales**	3. **TinderBox.com inc. - Sales proposal management service - storage and**

Department	A (Description)	B (Conditions)	C (Reasons)
	- storage and access - prospective client representative's business contact information (name, e-mail address) and proposal interaction analytics Pursuant to s. 5(2) PIIDPA the head of Nova Scotia Business Inc. (NSBI) determined the storage / access outside Canada of individuals' business contact information (name, e-mail addresses) and proposal interaction analytics information in NSBI's custody / control, as part of the sales proposal management services supplied under contract by TinderBox.com, Inc. (a US corporation based out of Indianapolis, Indiana) is to meet the necessary requirements of NSBI's operation.	**proposal management service - storage and access - prospective client representative's business contact information (name, e-mail address) and proposal interaction analytics** The individuals' business contact information (name, e-mail address) and proposal interaction analytics is to be protected in accordance with the TinderBox.com, Inc. service agreement, privacy policy and security statement which recognize NSBI as owner of the stored data, provides strong privacy protection and security processes and is EU Safe Harbour compliant.	**access - prospective client representative's business contact information (name, e-mail address) and proposal interaction analytics** NSBI requires a convenient and secure proposal management service for streamlining the creation, management, customization of NSBI sales proposals, value proposition and program / service promotional presentations for prospective business clients, that can be integrated with NSBI's Salesforce.com CRM service.
	4. **International In-market consultants - trade development & investment attraction services - storage and access - personal information (primarily business contact information)** Pursuant to s. 5(2) PIIDPA the head of NSBI determined the	4. **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	4. **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

Department	A (Description)	B (Conditions)	C (Reasons)
	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. 5. **NSBI directors, officers, employees - performance of duties during international travel - storage and access - personal information** Pursuant to s. 5(2) PIIDPA, 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.	agreement including confidentiality provisions. 5. **NSBI directors, officers, employees - performance of duties during 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 and Oath of Office and the NSBI Privacy Policy.	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. 5. **NSBI directors, officers, employees - performance of duties during 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	The NSLC did not make any decisions that resulted in the storage of personal information	N/A	N/A

Department	A (Description)	B (Conditions)	C (Reasons)
Corporation	outside of Nova Scotia in 2012. In prior years, we had made decisions that resulted in the storage of personal information outside of Canada which continue to this day. These have been reported in the year they occurred.		
Nova Scotia Securities Commission	During the 2012 calendar year, 11 staff members requested and received permission to take their BlackBerrys out of country while travelling on business and for pleasure. Staff members require their Blackberries to allow them to maintain contact with staff to deal with matters of urgency while away. One approved request was subsequently withdrawn and the device not taken.	Staff complied with the recommendation provided by the Chief Information Office regarding safe and secure transport and storage of portable storage devices. These devices are password protected. Remote access to GroupWise/Outlook is protected by Username/password authentication and is delivered over a SSL encrypted link via the secure government 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 matter. Many of the staff members work on administrative matters that require their immediate action or response, some staff members work on individual files and sit on various national and international committees working on time sensitive material and must be able to fulfill their responsibilities on behalf of the Commission.
Public Prosecution Service	One person traveled outside of Canada with a Blackberry and checked for work related messages.	The conditions placed on such access involved the use of encryption and password protection. The Blackberry was kept in custody of person during all times.	The Blackberry was password protected and was necessary to check for work related messages. Messages received were responded to and staff given directions as requested in a timely manner.
Public Service Commission	1. Five employees travelled outside Canada for business purposes with a Blackberry mobile phone. 2. The department internet site	1. The Blackberry device was password protected and was used for work related communication. 2. Google Analytics records the IP	1. The Blackberry was necessary to facilitate work related communication. 2. Analytical information allows the

Department	A (Description)	B (Conditions)	C (Reasons)
	employs Google Analytics to monitor web site traffic. Google Analytics is a service provided by Google, based in the USA.	address of a user, provided by their Internet Service Provider, as they access the site. The IP address is masked to provide partial anonymity by removing the last portion of the IP address.	department to monitor use of the internet as a communication and support channel for government employees, and the wider population.
Service Nova Scotia and Municipal Relations	The Interprovincial Record Exchange Program is a system that allows Canadian motor vehicle jurisdictions to securely query other jurisdiction's driver and vehicle records. The Canadian Council of Motor Transport Administrators (CCMTA) acts as the 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.	CCMTA acts as the clearing house for all queries so that jurisdictions do not have direct read access to another jurisdiction's system. Queries are forwarded to/from member jurisdictions only (CCMTA & AAMVA). Queries are pre-formatted and specific as to what information is displayed. CCMTA has contracts with each of its member jurisdictions that conform to the jurisdiction's privacy legislation concerning disclosure and consent	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.
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 the 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	In 2004, a tendering process was undertaken to purchase a new ticketing system. Paciolan was chosen as the bid winner as they could offer the best solution for our requirements. No vendor based in Canada could provide the same level of service necessary for our business. 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	

Department	A (Description)	B (Conditions)	C (Reasons)
	is under the ownership of TCL.	effective June 1, 2012.Legal council was sought on the original agreement and on the renewal in regard best practices and privacy requirements and the contract was found to be sound. 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 information on events etc. and only then will they be sent any correspondence outside the ticket purchase for which the information was supplied. Other 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.	

Department	A (Description)	B (Conditions)	C (Reasons)
Transportation and Infrastructure Renewal	1. When staff travelled outside of Canada a travel request form, prepared by staff and management, was approved by the DM prior to travel.. 2. There was no storage of personal information in the custody or control of the Department of Transportation and Infrastructure Renewal outside of Canada from January 1, 2012 to December 31, 2012.	1. Employees who requested permission to use their wireless devices who may have accessed personal information while outside Canada agreed to comply with the provisions of the Personal Information International Disclosure Protection Act (PIIDPA) - Section 5 & 9(4), as well as, comply with recommendations provided by the Chief Information Officer regarding safe and secure transport and storage of portable storage devices. Each year a memo is sent out to all TIR staff as a reminder of the legal requirement pertaining to the protection of personal information contained on electronic devices when staff are traveling outside Canada. Remote access to e-mail is protected by username/password authentication. All BlackBerry must be password protected and access to GroupWise/Microsoft Outlook system was protected by username/password authentication which is delivered over SLL/encryption.	Decision made to allow employees' access to GroupWise/Microsoft Outlook while outside Canada on business or pleasure was based on the need to maintain contact with department staff and to deal with matters of urgent need while they were away from the office. Access was granted to employees' who requested permission to use their BlackBerry or cell phone and or laptop to access their e-mails which had some contact information and may have accessed personal information through email through GroupWise/Microsoft Outlook. 1.

Department	A (Description)	B (Conditions)	C (Reasons)
Treasury Board	As part of the Treasury Board sponsored Spend Analysis and Strategic Procurement Project, a decision was made and documented via a Privacy Impact Assessment to allow the storage or access outside of Canada of limited personal information of Province of Nova Scotia employees. The data contained employees' travel-expense reimbursement information, as the data was necessary to develop a profile of government spending on travel.	All data are stored in a UK-based Oracle database residing behind Cisco firewalls. This non-US storage arrangement was negotiated to mitigate the potential negative impact of the US regulatory environment. The database is only accessible via the application logic tier. Users access the application across an encrypted connection. The information flow has been fully reviewed and validated by the Provincial IT Security Authority. In addition, the data will be stored on the UK server for up to one year, after which the data will be securely disposed of by the vendor at the direction of Treasury Board Office.	The decision to allow storage or access of the personal information outside Canada meets the necessary requirements of government operations, since without the data, it would have been impossible to develop a profile of government spending on travel in order to develop cost-saving strategies. The collection, use and disclosure of such employee information is necessary for payment-remittance as well as auditing purposes. Therefore, consent for the use of such information is implicit.
Utility and Review Board	The Board continues to use the Ceridian payroll service for its own employees.	The service provider has agreed not to store information outside of Canada.	No suitable compliant service provider has been found in Canada.
Workers' Compensation Board	1. **Employee Access to Personal Information by Mobile Device (IPhone, IPad, Blackberry) or computer (laptop, desktop)** - 25 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 or remote access. 2. **Employee Access to Personal Information by**	1. **Employee Access to Personal Information by Mobile Device (IPhone, IPad, Blackberry) or computer (laptop, desktop)** – 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 Remote Access Only** – Access to WCB's internal network is	1. **Employee Access to Personal Information by Mobile Device (IPhone, IPad, Blackberry) or computer (laptop, desktop)** – 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. 2. **Employee Access to Personal Information by Remote Access Only** – When staff travel for business purposes,

Department	A (Description)	B (Conditions)	C (Reasons)
	Remote Access Only – 598 individuals' personal information (contained in unique claim files) accessed from a remote location outside of Canada (in the U.S.) through a secure portal into the WCB;s internal network by remote access. 3. **Medical Consultant Access to Personal Information by Remote Access Only** – 18 instances of access to personal information (contained in unique claim files) accessed from a remote location outside of Canada (in the U.S.) through a secure portal into the WCB's internal network by remote access.	protected by username/password authentication and is delivered over a secure portal. Immediate report of theft/loss of device or information. 3. **Medical Consultant Access to Personal Information by Remote Access Only** – Access to WCB's internal network is protected by username/password authentication and is delivered over a secure portal. Information limited to only necessary medical information required to complete a review and provide medical report.	they are expected to monitor their email and voicemail for business continuity and to fulfill their job related responsibilities. 3. **Medical Consultant Access to Personal Information by Remote Access Only** – 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, 2012 Foreign Access and Storage by Health Authorities

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Annapolis Valley District Health Authority	1. **Contracts:** AVDHA was involved with 46 service contracts. None of these contracts allowed or required access or storage of personal information outside of Canada. 2. **Travel:** It is estimated that 12 AVDHA employees travelled outside of Canada. They may have accessed personal information via laptop, Blackberry or PDA's.	1. All new or renewed contracts have an inclusion clause added to contracts requiring vendors to comply with PIIDPA Legislation. 2. Laptops, Blackberry devices and PDA's are password protected. Laptops and removable USB storage devices are encrypted (mandatory). Blackberry devices also have an auto-wipe feature (mandatory). All staff who seek remote access to AVDHA computer systems must apply for remote access privileges and their devices are assessed to ensure they have the necessary security controls. 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.	1. Access and storage of personal information from 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.
Cape Breton District Health Authority	**1. Travel** - Approximately 7 employees traveled outside of Canada and may have accessed personal information via remote e-mail or		

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	Blackberry. 2. **Contracts –** Cape Breton District Health Authority entered into 16 maintenance contracts with the following vendors: Toshiba Canada for diagnostic imaging; Philips Medical for echo cardiography and diagnostic imaging; Fresenius Medical for renal dialysis; GE Health Care for diagnostic imaging, EKG, Lightspeed RT (CT scanner) and workstation; Varian Medical for radiation therapy; Dictaphone Solutions for dictation system; Quality America for Q-Pulse Software; Siemens Canada Limited for mammography, Viva E Analyzer, M248 Analyzers – IC, NS, Advia Centaur XP Immunochemistry Analyzer; Radiometer Canada for blood gas analyzer; Ventana/Roche for pathology Benchmark XT; Beckman Coulter for LH750 Analyzer; Biomerieux for Vitek 2 XL and Bact Alert 240 Analyzers; Ortho Clinical Diagnostics for Vitros Analyzers; BioRad for Variant II and Philips Healthcare for C-Arm, Infinia Hawkeye, Pegasys Ultra; and Sepmex for CBC Analyzers.	2. **Contracts** – All new and renewed contracts have inclusion clauses requiring vendors to comply with PIIDPA legislation.	2. **Contracts** – Current access to and storage of information outside of Canada is linked to pre-existing programs and/or systems utilized in the Cape Breton District Health Authority and deemed necessary for ongoing operations.
Capital Health District Authority	1. Vendors requiring access to personal information from outside of Canada are granted access on a need to know basis for the purpose of	1. PIIDPA compliance is a requirement in all new and renewed contracts where there is the potential for storage or	1. Current access to and storage of information outside of Canada is tied to pre-existing CDHA programs and/or systems that are necessary for

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	equipment and IT system maintenance as necessary for the operations of the health authority and when the expertise does not exist in house. 2. Staff members travelling outside of Canada may have accessed personal information via remote access or their Blackberry.	access of information outside of Canada. CDHA's Privacy Policy also applies. 2. Staff seeking remote access must apply for privileges and their equipment must have the required security controls as per the CDHA Remote Access Policy.	operations. 2. Staff members who are travelling may require access to personal information for the following purposes: patient care, business continuity and operational support.
Colchester East Hants Health Authority	Two people travelled outside of the country on District Health Authority business during 2012 who accessed personal health information while away.	The personal health information that they accessed was necessary for ongoing business purposes.	Only to access personal health information necessary for ongoing business purposes.
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. Decision regarding storage/access of personal information outside of Canada is pending upon future guidance: regulations, policies and	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 auto-wipe features.	Access and storage from outside of Canada are 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)
	procedures.	Established a process whereby all business changes that may affect the release, use or access to private information are reviewed regularly by the Privacy and Information Management committees. Privacy Impact Analysis must be completed on all new systems.	
Guysborough Antigonish Strait Health Authority	1. There are no records of personal information stored outside of Canada. 2. There were five staff members who used their Blackberries as telephones while away in the U.S. and one of them also checked emails but did not exchange emails containing personal identifying information.	2. Access to patient care systems are protected by a firewall managed by HITS NS. Access to these systems is controlled using VPN, therefore, upgrades or maintenance activities are managed by HITS NS.	1. No decisions were made. 2. Blackberries were used to stay in touch with the DHA.
IWK Health Centre	1. **Laboratory Testing:** IWK refers certain laboratory testing to laboratories outside of Canada if the specialized tests required are not offered in Canada, or the cost of having the tests performed in Canada are prohibitively high. IWK seeks referral laboratories in the USA first, and if the required testing cannot be performed at an American laboratory, European or Australian laboratories are secured. As per IWK Department	1. **Laboratory Testing:** Consent is obtained from patients wherever practicable prior to sending samples to be tested at laboratories outside of Canada. IWK Laboratory Services carefully tracks all external referrals, whether sent inside and outside of Canada. The Department of Pathology and Laboratory Medicine has a	1. **Laboratory Testing:** Obtaining certain specialized laboratory testing services from outside Canada is a necessary requirement of IWK's operations, as the IWK provides genetic testing for the Maritime Provinces. Genetic testing is an evolving field continually requiring increasingly esoteric testing.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	of Pathology and Laboratory Medicine policy, wherever possible, efforts are made to work only with referral laboratories that meet international standards with respect to the collection of information, collection of samples, and storage and retention of medical records. During the 2012 calendar year, IWK worked with 44 international laboratories (36 laboratories in the USA, 2 laboratories in Germany, 5 laboratories in the UK, and 1 laboratory in Norway) for the purpose of securing specialized and necessary laboratory testing.	Laboratory Standards Coordinator, responsible for monitoring referral laboratories for current accreditation and licensing/certification status, in accordance with the Department's Evaluation, Selection and Monitoring of Referral Laboratories Policy. New referral labs, and new testing sent to current labs, are submitted to the Laboratory Standards Coordinator for an assessment application process, and information regarding all assessed laboratories is maintained in an IWK laboratory database. The accountability for the non-Canadian laboratories selected lies with the IWK Clinical Division Head, Pathology and Laboratory Medicine. All laboratories are checked every 12 months for current accreditation status.	
	2. **Non-Canadian Contractors /Vendors with Remote Access:** IWK contracts with certain specialized service-providers who, in the course of providing their services, access remotely or store outside of Canada,	2. **Non-Canadian Contractors/Vendors with Remote Access:** IWK contracts with service providers where there is potential for storage of or access to personal	2. **Non-Canadian Contractors/Vendors with Remote Access:** The vendors IWK contracts with that store or remotely access personal information from outside Canada do so to deliver their

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	personal information in the custody and control of IWK. IWK's IT department facilitates the access, and HITS Nova Scotia provides VPN software on service providers' systems (all information accessed remotely is done via the encrypted HITS-NS Aventail VPN solution). When dealing with large vendors, Site-to-Site VPN access can be used. Terms of access are contractually controlled. 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	information outside Canada, then wherever practicable, IWK obtains individuals' consents or uses contractual conditions to protect privacy and confidentiality (including requiring vendors to agree to secure network access requirements, confidentiality clauses, and other accountability measures intended to safeguard personal information). IWK's Privacy Office oversees standard remote access given to vendors, and requires vendors to complete remote access forms to allow IWK to appropriately limit and control the type of access. In addition, 'Privacy Impact Assessments' (PIAs) are 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 sometimes used by IWK. Survey Monkey's	specialized services. Often these vendors are the only companies able to service or maintain the products IWK requires and uses in its day to day operations including specialized software and equipment.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		server is located outside of Canada (therefore, so is any data input into the tool). As such, 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 Privacy Office is required to access this tool on the IWK network.	
	3. **Business Travel:** During the 2012 calendar year, IWK's records indicate 117 incidents of travel booked through the IWK for work-related travel outside Canada, by 102 IWK staff members. During these incidents of international travel, personal information may not have been stored or accessed outside Canada, as staff usually do not require access to personal information in IWK's custody and control during such business travel. Further, staff typically do not transport personal information or access personal information on mobile devices, such as laptops, blackberries, iPhones and cell phones during such international travel rather the devices tend to be used only to maintain e-mail	**Business Travel:** If IWK staff members require access to personal information in the custody or control of IWK during international business travel, they are able to access IWK information systems via secure remote access connections. Staff are asked to log-in to these systems through protected remote desktop sessions/terminal services, which connect directly to the staff member's IWK computer. Further, laptops and handheld electronic devices are equipped with encryption software or are password protected, to protect information that is stored on the	**Business Travel:** The incidents of international business travel may not involve the storage or access of personal information outside of Canada. However, in the event such access/storage does occur, it is generally for the purpose of ongoing patient care or an ongoing healthcare research project.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	and/or phone contact with the IWK.	equipment, or that can be accessed with the equipment, from unauthorized access and disclosure. Staff are also advised to configure handheld devices so that email is not accessible (if not required). The telephone capabilities of the device can still be used. 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 are in place for Terminal Servers and Remote Desktop Stations. This software allows IWK network administrators to control what users can do during a remote session where the IWK network is accessed. For example, certain functions are controlled or prevented: copy/paste, remote printing and mapping of serial and printer ports. This software has the effect of turning a remote access session into a 'window' capable of viewing IWK information systems, while preventing information from being	

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		removed from the system. -IWK blackberries and staff phones are mandatorily password protected. A five minute period of non-use triggers the requirement to enter the password to unlock the device, and if a user fails to enter the correct password in a set number of attempts, the device is automatically wiped of its data/content. -IWK laptops 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 those laptops.	
Pictou County Health Authority	1. Access and storage from outside Canada is linked to pre-existing programs and / or systems utilized at PCHA which continue to be required to be used for the necessity in ongoing operation of these systems and programs (e.g. Meditech, Dictaphone, 3M). 2. PCHA Leaders have accessed personal information while conducting business outside the country using remote e-mail and Blackberry.	1. Vendors and staff are required to follow PIIDPA legislation. 2. Staff are required to follow PCHA's privacy policies, including guidelines around accessing remote e-mail and Blackberry service out of	1. Access and storage from outside Canada is linked to pre-existing programs and / or systems utilized at PCHA, which are required for ongoing operations of these systems and programs

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		country.	
South Shore District Health Authority	Between January 1, 2012 and December 31, 2012 there were two SSH employees who travelled outside Canada who had the ability to access personal information either via laptop or blackberry. Both employees had approval from the CEO.	Policies exist covering restrictions. All laptops, blackberry devices are password protected. Laptops and removable USB storage devices are encrypted. Blackberry devices also have an auto-wipe feature.	Policies exist supporting decisions.
South West Nova District Health Authority	1. No SWH employees were involved in international travel where they maintained access to the organization through cell / blackberries. SKYPE access was set up on one computer in the Veterans Unit for humanitarian reasons. 2. In 2012, SWH entered into service agreements for the following vendors/instruments/models: Lab Biomerieux Inc./Vitek.2-60 Fisher Scientific/Cryostat956634DH Radiometer/ABL825 Simmens/Clintek Atlas(SSH/MammomatInspiration DA-YARMO-007922 Somagen Diagnostics/Tissue-Tek VIP 5 Bench Respitatory Cardinal Health Canada(source) Health Information Nuance Communications/ transcription services Diagnostic Imaging Philips Medical	2. The district continues to add the inclusion clause re the management of the information in all requests for proposals, new contracts, warranties or renewals.	2. SWH uses software vendors located outside Canada who maintain systems remotely; for example Meditech (Health Information); SAP (financial & 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.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	Systems/Duo Diagnost 527066		

Table 3[2]: January 1 - December 31, 2012 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 the CBU system.	1. **Alumni / Donor Database:** Access is restricted to authorized technical support carried out by working with a CBU employee, possibly online. Access to this information is authorized for the purpose of required assigned duties and research.	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:** CBU faculty may access portions 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 of time grades are submitted or by a faculty teaching a distance program. As well, students have web access to the Student Information System to view their individual financial and	2. **Student Information System:** Access to student records is restricted to those employees in positions requiring access to fulfill their job requirements at the university and is managed through authorized user accounts. Student access is limited to viewing their own recorded information and is managed through authorized student accounts. All access is authenticated and all transactions are encrypted.	2. **Student Information System:** The system is required to meet the operational requirements of the University.

[2] Acadia University and Nova Scotia Agricultural College reported that they had no foreign access or retention of personal information outside of Canada.

Universities	A (Description)	B (Conditions)	C (Reasons)
	academic records. 3. **Course Management System:** CBU uses MOODLE as its course management system. The system facilitates online 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. 4. **Travel:** Approximately 47 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 assigned duties or as a necessary part of a research project.	3. **Course Management System: 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 and student postings. Student access is restricted to students registered in a particular course, is authenticated and encrypted. 4. **Travel:** Web access to travelling employees is restricted to email and is available to authentication users only. Access to CBU systems is authenticated and transmissions are encrypted.	3. **Course Management System: Moodle** – The 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 positions.
Dalhousie University	1. **Plagiarism Detection:** Academic programs: Online plagiarism detection service (storage in US).	1. **Plagiarism Detection**: Technical security measures: data security controls in place. Contractual security measures: restrictions on access to and disclosure of information by	1. **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

Universities	A (Description)	B (Conditions)	C (Reasons)
		service provider and their employees; Internal security measures: process in place to minimize disclosure of personal information.	controls in place. Minimal personal information disclosed.
	2. **Clinical Experience Software:** Software for tracking anonymous student clinical experiences and feedback.	2. **Clinical Experience Software:** 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.	2. **Clinical Experience Software:** 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.
	3. **Student Engagement Survey:** Student survey about academic experience of law school students.	3. **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.	3. **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.
	4. **Crowd Sourcing Product:** Online tool to post questions	4. **Crowd Sourcing Product:** Technical security measures: hosted in a secure server	4. **Crowd Sourcing Product:** Improves efficiency in asking and responding to

Universities	A (Description)	B (Conditions)	C (Reasons)
	and answers relating to information technology services.	environment that uses firewall, encryption; Internal security measures: restricted access, minimal disclosure of personal information.	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.
	5. **Campus Recreation Impact Study:** Student survey to measure student athletic facilities experiences.	5. **Campus Recreation 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.	5. **Campus Recreation Impact Study:** Necessary to assess the quality of athletic 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.
	6. **Hosted Learning Management System:** Academic product used extensively by faculty for online teaching.	6. **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.	6. **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.
	7. **Maintenance Support for**	7. **Maintenance Support for**	7. **Maintenance Support for Student Learning Outcomes Software:** Relates

Universities	A (Description)	B (Conditions)	C (Reasons)
	Student Learning Outcomes Software: Academic product used by Faculty of Engineering to plan, implement and measure student learning outcomes supporting curriculum objectives and graduate attributes.	**Student Learning Outcomes Software:** 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.	to larger effort at curriculum mapping and assessment with engineering and pending changes to accreditation process. There is currently no comparable product offered in Canada. Access controls in place.
	8. **Maintenance Support for Environmental Health and Safety Database:** Software system to track and monitor environmental health and safety incidents.	8. **Maintenance Support for Environmental Health and 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.	8. **Maintenance Support for Environmental Health and Safety Database:** Software system necessary to adequately track and monitor incidents, superior functionality and support than competitors. Access controls in place.
	9. **Maintenance Support for Online Exams:** Software to administer online law school exams.	9. **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.	9. **Maintenance Support for Online Exams:** Specialized software used exclusively in law schools in Canada, US and UK. There is currently no comparable product offered in Canada. Access controls in place.
	10. **Financial Services:** Service provider for the creation of templates for various electronic financial services, e.g., purchase orders,	10. **Financial Services:** Limited access: only where required for maintenance and troubleshooting. Personal information stored internally.	10. **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

Universities	A (Description)	B (Conditions)	C (Reasons)
	bills, cheques, etc.	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.	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.
	11. **University ID Card:** Management of access and financial processes used through the University ID Card.	11. **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 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.	11. **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 function of the University.
	12. **Employment Tool:** Comprehensive online tool to	12. **Employment Tool:**	12. **Employment Tool:** Providing tools for students to develop job-seeking skills

Universities	A (Description)	B (Conditions)	C (Reasons)
	assist students in seeking employment.	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.	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.
	13. **Network and System Upgrade:** Consulting services related to the University's ongoing upgrade of its internal network and systems.	13. **Network and System Upgrade:** Limited access: only where required for maintenance and troubleshooting. 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 functions and pre-approved IP addresses.	13. **Network and System Upgrade:** Consultant services, provided by the current provider of the systems, are being upgraded and thus have the expertise to provide the services required. These systems are necessary for the operation of integral Dalhousie computing services.
	14. **Wireless Products:** Service provider for wireless products for employees, long	14. **Wireless Products:** Contractual security measures: restrictions on access to and	14. **Wireless Products:** Mobile communications solution for employees as well as long distance calling and

Universities	A (Description)	B (Conditions)	C (Reasons)
	distance and teleconferencing services.	disclosure of information by service provider and their employees. Internal security measures: process in place to minimize disclosure of personal information.	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.
	15. **Warranty Maintenance:** Product warrant maintenance for electronics (storage in US).	15. **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 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.	15. **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.
	16. **Maintenance support** for product will allows University staff and faculty to schedule and manage meetings and activities in an integrated environment (remote access for maintenance from US).	16. **Maintenance Support:** Contractual security measures: restrictions on access to and disclosure of information by service providers and employees; remote access to university systems will be subject to Dalhousie protocols	16. **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.

Universities	A (Description)	B (Conditions)	C (Reasons)
		including time restrictions, audit function and pre-approved IP addresses.	
	17. **Maintenance support** for academic product used extensively by faculty for online teaching (remote access from US).	17. **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.	**17. Maintenance Support:** The provision of online teaching opportunities is necessary to Dalhousie academic operations. This product offers a superior range of services and functionality and has been an established service at Dalhousie for several years, therefore, would require a heavy cost to convert; access rarely required.
	18. **Maintenance support** for statistical software product used in course teaching and research (remote access from US).	18. **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. 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	18. **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.

Universities	A (Description)	B (Conditions)	C (Reasons)
		purposes.	
	19. **Academic software:** supports teaching activities and allows for online collaboration, e.g., voice, video, application sharing, etc. Information stored on the server is 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 integrated with other existing University applications (access from the US).	19. **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 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.	19. **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 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.
	20. **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	20. **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	20. **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.

Universities	A (Description)	B (Conditions)	C (Reasons)
	the US.	audit function. Where possible, personal information will be removed from products which require service.	
	21. **Maintenance support** for a web-based database that manages information and processes related to student work experience placements in industry (remote access from US).	21. **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.	21. **Maintenance Support:** Effectively managing information and processes for student work placements is necessary for the operation of Dalhousie co-operative education programs particularly in Architecture, Commerce, Computer Science and Engineering. Cost prohibitive for Canadian alternative; access rarely required.
	22. **Maintenance support** for product which allows for real-time synchronization of faculty and staff calendars with wireless tools (remote access from US).	22. **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.	22. **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.
	23. **Plagiarism Detection:** Academic program: online plagiarism detection service (storage in US).	23. **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	23. **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.

Universities	A (Description)	B (Conditions)	C (Reasons)
		segregated from other users; internal security measures: process in place to minimize disclosure of personal information.	
	24. **Maintenance support** for product which supports all major University administrative computing applications (remote access from US or Bangalore, India).	24. **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.	24. **Maintenance Support:** Necessary service for the operation of integral Dalhousie academic computing services; no Canadian alternative identified; access rarely required.
	25. **Maintenance support** for facilities management product used for reserving rooms on campus specifically for event and classroom scheduling (remote access from US).	25. **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.	25. **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.
	26. **Maintenance support** for academic product which provides students with information regarding their progress towards meeting their	26. **Maintenance Support:** Contractual security measures: restrictions on access to and disclosure of information by	26. **Maintenance Support:** Allowing students to access their information regarding progress towards degree requirements is necessary for Dalhousie

Universities	A (Description)	B (Conditions)	C (Reasons)
	degree requirements (remote access from US).	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.	operations particularly in student advising and counseling and for the Registrar's Office. No Canadian alternatives have been identified; access rarely required.
	27. **Maintenance support** for a scheduling and data tracking software designed for university student advising and counseling (remote access from US).	27. **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.	27. **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 services; access rarely required.
	28. **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).	28. **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.	28. **Maintenance Support:** The ability to identify and address potential student performance issues at the earliest possible stage is necessary for Dalhousie operations in terms of enhancing student experience. No Canadian alternatives identified; access rarely required.
	29. **Evaluations:** Software product used to collect and maintain evaluations	29. **Evaluations:** Data is stored internally. Contractual security measures: restrictions on access to and disclosure of information	29. **Evaluations:** Medical education evaluations are a necessary requirement of the operation of our Faculty of Medicine; proper management of these

Universities	A (Description)	B (Conditions)	C (Reasons)
	specifically in the medical education field (e.g., student evaluations, preceptor evaluations, etc.). This product was originally developed in Canada, however, is now a wholly-owned subsidiary of a US company. Product is still maintained in Canada.	by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, pre-approved IP addresses and segregation of personal information where possible. Vendor agrees that any remote access will only occur from within Canada.	evaluations is critical to decision-making with respect to promotion throughout a student's medical education. This tool was 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.
	30. **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).	30. **Academic Software:** Contractual security measures: restrictions on access to and disclosure of information by service provider and employees.	30. **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.
	31. **Hardware/Software:** Lease and maintenance multifunction devices (copy / print / scan / fax devices). Vendor headquartered in Japan.	31. **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	31. **Hardware/Software:** No Canadian alternatives identified. Awarded through a tender process.

Universities	A (Description)	B (Conditions)	C (Reasons)
		communication; limited outbound destinations; prohibited inbound connections; internal administrative controls to limited access to personal information.	
	32. **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.	32. **Website Feedback:** Restricted access through server authentication and data encryption and no IP logging.	32. **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.
Mount Saint Vincent University	1. Storage Outside Canada: The University did not store any information such as employee data, student records or other personal information outside Canada. 2. Access from Outside Canada: Students, faculty and staff (whether travelling or living) outside Canada were granted access to email accounts and information systems stored on servers within Mount Saint Vincent University (and within Canada) via email or remote access systems using appropriate	2. There was no limit in the amount of information that a student, faculty or staff member could access from outside Canada within their access rights. The information they have access to is maintained on a server controlled by Mount Saint Vincent University (within Canada).	2. 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 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

Universities	A (Description)	B (Conditions)	C (Reasons)
	authentication credentials.		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 Community College	1. As required by Section 5(3) of the *Personal Information International Disclosure Protection Act*, the 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, US. Hobsons EMT is an application service provider offering web-based data	1. The services of Hobsons EMT are required to support the application process for many of our student applicants. 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.	1. Since our last submission (March 21, 2012), we investigated service providers within Canada, however, there were no emerging or known Canadian companies identified by us through the usual channels, i.e., conferences, trade shows and vendor contacts. The College is currently in the process of exploring the on-line application solution through our current database service provider (Oracle/PeopleSoft) and is estimated to have this solution implemented by September 2014.

Universities	A (Description)	B (Conditions)	C (Reasons)
	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 2012, the College implemented a Status Solutions LLC life safety project (Situational Awareness and Response Assistant). Status Solutions LLC is headquartered in Charlottesville, VA in the US.	2. The installation is locally hosted and maintained in Nova Scotia. However, consultants located in Ohio, US were accessing information while assisting with the system setup and configuration. Access is provided in a secure manner and was specifically limited to the life safety project. No data was sent outside of Canada.	2. Access to the system will be rescinded upon completion of the project.
	3. The College will allow employees to transport personal information temporarily outside Canada but only to the extent that it is strictly necessary for their assigned duties or as a necessary part of a research project. We anticipate that this information will be transported using cellular telephones, wireless handhelds, laptops and storage devices.	3. Employees will be required to take all reasonable precautions (e.g. encryption) to protect the personal information. 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/her assigned duties or as a necessary part of a research	

Universities	A (Description)	B (Conditions)	C (Reasons)
		project.	
NSCAD University	No storage or access permitted outside Canada in calendar year 2012.	Access to personal information from outside Canada is limited to escalated support calls where only trained vendor technologists are capable of performing the required tasks and occur only with the expressed permission of the Director of Computer Services.	Access to personal information from outside Canada is permitted only in situations where alternatives are not 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.
St. Mary's University	1. **Plagiarism Detection:** Academic program: online plagiarism detection service (Storage in US.) 2. **Maintenance Management System:** The software is a Maintenance Management System that acts as the requesting system for identified key users on campus and the issuing and tracking of work request and preventive maintenance work for all building on campus. 3. **Travel:** Members of the University travelling outside	1. **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. 2. 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. 3. Employees will be required to take all reasonable	1. 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. 2. This system is required to meet the operational requirements of the university. 3. Remote access to email is required by employees to meet the operational

Universities	A (Description)	B (Conditions)	C (Reasons)
	the country have access to their personal email via smart phone or laptop. 4. **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.	precautions (e.g. encryption) to protect personal information. 4. Limited access to 10 Facilities Management office staff and thus hold their e-mail address.	requirements of their positions. 4. This software is a common system used by all Atlantic Canada universities and most universities across Canada.
St. Francis Xavier University	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 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.	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 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.	1. The cost of switching our software vendors is cost prohibitive at this time and Bi-Tech provides the support required for efficient and secure operation.

Universities	A (Description)	B (Conditions)	C (Reasons)
	2. Kinetics software (Kx) is a comprehensive software program that manages catering, facility and residential bookings. It is comparable to large conference or hotel management systems. The Conferences and Special Events Department uses the program 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. 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.	3. 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 set up with a user account has access to data based on role and permission settings. Access is limited to need of role.	3. Data for our EZ Facility account is stored and managed within the Rackspace Data Centers in their Chicago, IL data center. Both Rackspace and EZ Facility are PCI Level 1 certified (highest possible), which is the Payment Card Industries global standard for data security. This involves tracking and permission limits to accessing account data and personal information. Hosting an application on our own servers was not a viable option at the time of purchase (and is still not).
	4. Due to web support and maintenance expertise that could not be performed in-house, the decision was made to have the StFX.ca website	4. Collected information is stored on the Acquia.com servers for a short period until St. FX employees download and	4. The technical expertise to host and support StFX.ca content management system was found with the named

Universities	A (Description)	B (Conditions)	C (Reasons)
	hosted by a US based company called Acquia. The company was selected based upon their expertise with the content management software that StFX.ca was built upon.	delete the information housed in Acquia. Employees log in to servers with user names and passwords and, thus, this information passes through the servers but is managed and stored within servers at St. FX not on Acquia.com servers.	company and not found within Canada.
Université Sainte-Anne	Université Sainte-Anne's student information management system is maintained by a US company called Blackbaud. Storage of the data-base is in the U.S.	Use of the data is restricted to Université Sainte-Anne as the user and to Blackbaud as the service provider. Distribution to third parties is not permitted unless under a lawful obligation to do so.	Hosting services are not available in Canada by the service provider. Legal counsel was obtained to ensure the Université met the PIIDPA requirements prior to giving consent.
University of King's College	Access to personal information in the custody or under the control of the University of King's College by its employees may have occurred from time to time remotely from locations outside Canada during 2012. A draft policy governing such access had previously been circulated within the university, and it is understood that faculty have been briefed on the policy. Access in accordance with the draft policy is accepted by the University of King's College as appropriate. The draft policy is in the process of being updated and reviewed for	See provisions 11 through 14 of King's draft privacy policy. http://www.ukings.ca/files/u42/Kings-Privacy-Statement-FINAL.pdf	Access outside Canada to personal information in the custody or under the control of the University of King's College, under the draft policy, is only permitted when necessary for the performance of the employee's duties. Without such access, employees would not be able to meet the requirements of their employment. The draft policy also notes that: "Employees must take reasonable precautions to protect the information. For instance, laptops should be secured against theft when travelling and employees should avoid submitting marks or accessing students' personal information online while outside the country."

Universities	A (Description)	B (Conditions)	C (Reasons)
	final approval. University employees may have stored personal information in the custody or under the control of the University of King's College on their laptop computers when travelling outside Canada where necessary for the performance of their employment duties. Storage is also understood to be generally in accordance with the draft policy. To the best of our knowledge, no other storage of personal information exclusively in the custody or under the control of the University of King's College occurred during 2012. Access and storage of personal information in the custody or under the control of the University of King's College may also have occurred through the use of employees of webmail accounts (e.g., gmail, hot mail, simpatico, etc. However, we have been advised with respect to faculty that "very little personal information is relayed through email, stored in the G drive or in cloud applications. Most		

Universities	A (Description)	B (Conditions)	C (Reasons)
	personal information resides in Blackboard, a service provided by Dalhousie University." Because of the integration of some of the University's information technology services with Dalhousie University, the University of King's College makes no representations with respect to any of its information stored on, or process through, Dalhousie University servers.		

Table 4[3]: January 1 - December 31, 2012 Foreign Access and Storage by School Boards

School Boards	A (Decision)	B (Conditions)	C (Reasons)
Annapolis Valley Regional School Board	AVRSB is one of seven Nova Scotia school boards using the Aesop system for 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, Ontario. The system is accessed remotely by schools and school board staff using the internet and a telephone Interactive Voice Response system. The system is supported and maintained by FTC's parent company, Frontline Placement Technologies (FPT) which is located in 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,	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. • FTC contracts data centre services with SunGard Availability Services for housing school board data and the Aesop system at their Toronto 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.	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 NS privacy legislation as well as housing the data and system in Canada.

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

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	2007.	• All equipment used for Aesop implementation in NS 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 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 School Board has contracted the services of Frontline Technologies Canada Inc. (FTC) for the scheduling and placement of substitute teachers and varying non-teaching classifications in schools in response to filling casual teacher and non-teaching absences. The Aesop System provided by FTC is an automated tool used for tracking, processing and storing information related to teacher absences. FTC utilizes an	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	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

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	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 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	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 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.	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 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

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	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. Effective 2012/2013 school year, this AESOP system was expanded in the Cape Breton-Victoria Regional School Board to also include the cleaners and Lunch/Bus/Ground supervisors.	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. 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.	privacy legislation as well as housing the data and system in Canada. 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 (FPT) are restricted to specific purposes and logged and reported to DOE monthly.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	2. Approximately 5 staff members travelled outside Canada and may 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.	2. Functionality of the operations of the board are deemed necessary for management and operations. The staff members at issue occupy management positions and must be available by email. **Provincial Student Information System** – 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. **Teacher Certification Fee Processing** – Teacher Certification offers the option of payment by credit card payments as a convenience for teachers and to provide efficient

School Boards	A (Decision)	B (Conditions)	C (Reasons)
			and effective online services. **<u>Teacher Summer Professional Development Application</u>** – The option of payment by credit card payments as a convenience for teachers and to provide efficient and effective online services. **<u>Travel with Electronic Devices</u>** – Staff are sometimes expected to monitor their email and voice mail for business continuity purposes and maintain contact with operations. Blackberries were necessary to make calls, access email and internet sites and make telephone calls. Laptops are needed for preparing documents, accessing email and internet sites.
Chignecto-Central Regional School Board	1. The Chignecto-Central Regional School Board (CCRSB) 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,		

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	determine which substitutes could be used for selected vacancy and contact substitutes manually by phone to fill the absences. As a result, CCRSB 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. The Aesop System provided by FTC is an automated tool used for tracking, processing and storing information. The DOE and seven school boards signed a five year contract in May 2008 – 2013 (it is currently in the process of being renegotiated). The system is supported and maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from CCRSB and to maintenance and support.		
	2. A number of CCRSB employees traveled outside of Canada and had the ability to access personal information contained in email or stored in the GroupWise email	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

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	system using devices such as the Blackberry, laptops, tablets and IPads. 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 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.	necessary for them to check email remotely. 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 leading distributor of the SIS software worldwide.
Halifax Regional School Board	Eight staff members travelled outside of Canada who would have had access to personal information via their smartphone or laptop computers.	Relevant HRSB policies would apply to Blackberry, IPhone and computer usage outside of Canada. Each smartphone and computer is password protected.	The staff members involved occupy positions where they must be available by email for decision-making, information and safety purposes.
South Shore Regional School Board	1. **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	1. **Tech Support:** For all the above 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 of the troubleshooting process, tech support outside Canada will connect via a remote desktop session. For such sessions, a one-time use	1. **Tech Support:** All above hardware / software is deemed necessary for the daily operations of the SSRSB.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	appliance, Taleo (web-based application for employment / hiring) and PHD virtual back-up software (application support). 2. **Travel:** Use of laptops and Blackberries outside of Canada. A number of SSRSB employees accessed their webmail or used their phones in a number of countries.	password or session ID is provided. Once the remote desktop session was ended / closed, outside tech support can no longer access our systems. 2. **Travel:** If deemed necessary for employees role, laptops, IPhones, IPads, tablets and Blackberry usage is allowed outside of Canada. All devices are password protected.	2. **Travel:** When deemed to be necessary for employees' role. Staff members at issue are in management roles and their availability via email and phone are for information purposes and decision-making.
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 employees (janitors, cleaners and building operators) absences. FTC 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	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 the Department of Education 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 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). FTC 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	

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	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 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.	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 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 OSO 9001:2000 certified by Lloyd's Registry Quality Assurance. All equipment used for the Nova Scotia Aesop implementation	

School Boards	A (Decision)	B (Conditions)	C (Reasons)
		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 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 Reading A to Z. These are on line subscriptions to education media. The teacher's name and school are provided to both online education media providers. This contract was		

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	in existence prior to December 15, 2006. 3. Regarding employees who travel outside of Canada, to our knowledge fifty three (53) have accessed via remote email. The Board has restricted employees who travel outside of Canada with Board owned equipment unless prior written consent of the Head of the Public Body is provided.	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 NotesTraveler 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.	3. Consent to transport Board owned equipment outside of Canada is provided only in instances when it is deemed necessary for management and operations. During 2012, one employee was granted permission to transport a Board Owned BlackBerry. The employee was travelling for the NS International Student Program. The decision was based on the necessity for the employee to contact parents of exchange students involved with NSISP in the event of an emergency. The BlackBerry was password/pin protected.

Table 5 January 1 – December 31, 2012 Foreign Access and Storage by Municipalities[4]

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
Halifax Regional Municipality	1. Between January 1st and December 31st, 2012, twenty-seven (27) HRM 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. HRM 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 system and software 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, HR and Crystal Reports), ESRI (GIS), IVOS (Risk Management), Track It (Help Desk), VTC (Metro	2. Vendor access is controlled and monitored by ICT Support staff.	2. Vendor access is necessary for systems to continue to function properly.

[4] Strait-Highlands Regional Development Agency, Cumberland Economic Regional Development Association, Halifax Regional Library, Region of Queens Municipality, South Shore Public Libraries, Cumberland Joint Services Management Authority, Lunenburg/Queens Regional Development Agency, Cape Breton Regional Municipality, Municipalities of the Counties of Annapolis, Antigonish, Cumberland, Inverness, Pictou, Victoria, Municipalities of the Districts of Argyle, Clare, Digby, East Hants, Guysborough, West Hants, Barrington, St. Mary's, Towns of Annapolis Royal, Berwick, Bridgewater, Clark's Harbour, Digby, Hantsport, Lockeport, Lunenburg, Middleton, Mulgrave, Oxford, Pictou, Port Hawkesbury, Shelburne, Springhill, Stellarton, Stewiacke, Trenton, Truro and Wolfville had no access or storage outside of Canada to report.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	Transit), Messaging Architects (Email Archive), Niche (Digital Mug Shot) - were provided access on an approved, need basis to the applicable production systems for support and maintenance. 3. **Service Providers** - Scotiabank and Merchant Card Services partner, Chase Paymentech were secured to provide Banking Services for the municipality for a five year period and Scytl was secured to provide electronic voting for the 2012 municipal election.	3. **Service Providers:** Service providers are bound by duly executed agreements that detail their obligations for the protection, use and disclosure of personal information.	3. **Service Providers:** Service providers were secured through the RFP process and achieved the highest overall proposal evaluation scoring and provided the best financial value for the municipality.
Halifax Regional Water Commission	1. Thirty eight staff were permitted to transport personal information devices such as laptop computers, cell phones and electronic data storage devices outside Canada sixty-seven times. 2. The following vendor, Tokay Navigator Software, Framingham, Massachusetts, provides initial customer data	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. Vendor access is controlled through a secure network portal (no direct link to support customer account information located in SAP). 2. Customer technical services are provided for in the annual agreement.	1. 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 requirements. 2. Vendor access is crucial to manage the Cross Connection Control Program.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	conversion and upload, periodic software maintenance and upgrades, and customer technical support.		
Municipality of the County of Colchester	Nine staff members travelled outside Canada during calendar 2012. It is known that three staff accessed personal email or stored information and email either through GroupWise / Outlook 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 Chester	Business purposes, technical and server support (occurred four times).	N/A	The nature of the access was required to fulfill business obligations of the Municipality.
Municipality of the District of Lunenburg	1. One Municipal Elected official travelled outside Canada and had the ability to access personal information via one or more of the following devices: Blackberry or I-Phone. Appropriate permissions were granted. 2. Municipal property owners living outside Canada are sent property	1. Official has been advised that the use of communication device that can gain access to personal information, to limit email use during the time out of the country. Prior to travelling, they are required to report their intentions to the PIIDPA administrator to ensure secure login/passwords and or encryption protocols are in place. 2. Email activity is controlled and monitored by our IT support.	1. Municipal Official was expected to monitor email in order to fulfill responsibilities / requirements. 2. This is an operational process that occurs on a regular basis

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	tax invoices twice a year (April and September). There are often exchanges in communication via email with these customers. 3. The following vendors were provided access on an approved, need basis to the applicable production systems for support and maintenance: (Townsuite/Procom - Taxes/payroll/financial operations, Digital Fusion - Website Administration, Land Development /HFX Support - Permit Tracking system, Atlantic Data Systems Support (FUNDY) - Municipal Servers and operating systems, Office Interiors - Photocopiers and Printers, Active Network Ltd. - Recreation and Golf Course Program Payment system).	3. Vendor Access is controlled and monitored by IT Support systems.	and provides for an efficient manner for customer service. 3. Vendor access is necessary in the daily operations of the municipality in order to continue business functions properly.
Municipality of the District of Yarmouth	One employee travelled to the US and had the ability to access personal information via one or more of the following means: cell phone, Blackberry & laptop.	All devices were password protected and the laptop information was encrypted. Access to our network was through our VPN.	When staff travel outside the country for business, training or pleasure, they may be required to monitor their email and voicemail to deal with urgent ongoing matters. Therefore, it is necessary for them to work

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
			remotely, where possible, in order to fulfill their responsibilities.
Property Valuation Services Corporation	PVSC uses 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 only 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.
Town of Amherst	Nine staff travelled outside Canada during the calendar year 2012 and had the ability to access personal information via cell phone or IPad.	Email access requires authentication through secure login/password.	Senior staff are travelling for business or personal reasons. They may be expected to monitor their business email in order to fulfill their job responsibilities.
Town of Antigonish	N/A	Personal information is stored on a server in our building with back up in Canada.	N/A
Town of Bridgetown	Since 2005, the website and e-mail for the Town of Bridgetown has been facilitated by a private firm, which has been hosted in Texas at the largest and most reputable web host. Only recently (2012) was e-mail moved to an in-house server. This will be followed soon by the website itself being moved to a Canadian-based	N/A	The decision to allow the Town's website and e-mail to go through a host server in Texas was made well before my employment with Bridgetown. Once it was identified, the e-mail was moved to a Canadian host and the website is in the process of being moved to a Canadian host as well.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	host. Besides e-mail, no other personal information was stored on the US-based server.		
Town of New Glasgow	Several employees within the Town of New Glasgow travelled outside of the country with their Town owned electronic devices which had been requested and approved by their Supervisor and CAO based on their job role within the Municipality. During this time, employees had access to the Town's email system from their Blackberry devices.	Blackberry devices are encrypted and also have a device password provisioned. Remote access to webmail is encrypted with SSL and protected with usernames and passwords which are changed on a regular basis.	Employees or Elected Officials from the Town of New Glasgow may request to travel out of the country with their Town provided electronic devices. A process has been put in place where the user must fill out a form and submit to their department head / supervisor to request permission to travel outside of the country with a Town provided electronic device. Final decision remains with the Chief Administrative Officer. The CAO will review the request from the employee and decide based on their job role within the Municipality if it is necessary for the user to travel with the device; such as senior staff within the Municipality and senior officers within the Town's Police Agency.