Personal Information International Disclosure Protection Act

2010 Annual Report

NS Information Access and Privacy Office
October 2011

Message from the Minister of Justice

I am pleased to provide the fifth Annual Report regarding public body decisions to permit foreign access and storage of personal information, as authorized under the *Personal Information International Disclosure Protection Act* (PIIDPA). PIIDPA was created to enhance provincial privacy protection activities and respond to Nova Scotian concerns about the vulnerability of public sector and municipal personal information holdings to foreign access, storage and disclosure. The Act prohibits public sector entities, municipalities and their service providers from allowing foreign storage, disclosure or access to personal information, except to meet the "necessary requirements" of a 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, 2010 to December 31, 2010 to the Minster of Justice. This report is based on the PIIDPA reports received by Nova Scotia Information Access and Privacy Office.

This report contains a summary of the 53 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: 67 entities reported that there was no access or storage outside of Canada for the 2010 calendar year.

Original signed by the Minister

The Honourable Ross Landry

Minister of Justice and Attorney General

Contents

Key to Columns in Submitted *PIIDPA* Reports

A: Description of the decision of the public body to allow storage or access of personal information in its custody or under its control outside Canada.

B: Conditions or restrictions that the head of the public body has placed on such storage or access of personal information outside Canada.

C: Reasons resulting in the head of the public body allowing storage or access of personal information outside Canada to meet the necessary requirements of the public body's operation.

Table 1: January 1 – December 31, 2010 Foreign Access and Storage by Government Departments, Agencies, Boards & Commissions [1]

Department	A (Description)	B (Conditions)	C (Reasons)
Agriculture	Investment Attraction - new entrants. Google Applications (analytics and mapping) are used as a website statistics and tracking software program. Google tracks website visitors via IP address and stores this information on servers located outside of Canada. Google Applications are used because they are user friendly and easily recognizable to the international client base the program focuses on attracting to Nova Scotia.	Investment Attraction - new entrants. The IP addresses are stored as part of the regular accounts being set up with Google Applications. We are not able to place any restrictions or conditions on the storage or access to this information outside of the company's regular privacy standards/set-ups.	Investment Attraction - new entrants. Individual IP addresses stored by Google Applications cannot be tracked back to an individual or location without the aid of the Internet Service Provider. This information is not released by an Internet Service Provider, except under extreme circumstance such as a court order. Therefore, it was decided that using Google Analytics is acceptable.
Chief Information Office (OCIO)	1. Symphony Services, located in California, was awarded a contract in 2006 by the Province of Nova Scotia (PNS) to supply and support an Expense Management System (EMS) which is used by the Infrastructure Service Management Group to re-bill, on a monthly basis, all telecommunication costs to PNS users. A report was filed by the	1. Microsoft's Terminal Services allows Symphony Services to view the PNS database used by EMS to store personal information. However, it does not give Symphony Services the ability to remove or copy any files. Once Symphony Services work is completed, its access to the database is disabled by PNS and is only re-enabled by PNS during scheduled support services or troubleshooting work. Under the agreement with PNS,	1. The EMS solution was selected by PNS because Symphony Services was very familiar with the PNS telephone billing requirements (it had previously supplied both Tru Server and TIMS). Symphony Services has successfully migrated PNS data from Tru Server to EMS and its prior experience lowered the risk associated with the migration of data. There is currently no alternative method of support access for EMS within

[1] Aboriginal Affairs, Auditor General, Emergency Management Office, Human Rights Commission, Public Service Commission, Office of Acadian Affairs, Seniors, Waterfront Development Corporation reported that no personal information was accessed or retained outside of Canada.

Department	A (Description)	B (Conditions)	C (Reasons)
	Minister of The Chief Information Office pursuant to subsection 5(3) of the Personal Information International Disclosure Protection Act (PIIDPA), with respect to the award of the contract to Symphony Services in 2006. PNS subsequently renewed the contract in 2010 to permit Symphony Services to continue to provide support services for EMS. In the course of providing services, Symphony Services at times requires access to the EMS application and database in order to do scheduled support or troubleshooting work. This access is done through its office located in Dallas Texas, and is executed remotely, using Microsoft's Terminal Services on a server located in the PNS data centre. Microsoft's Terminal Services provides three levels of authentication and is only made available by PNS to Symphony Services during scheduled times. When access is provided to Symphony Services it is monitored by PNS employees.	Symphony Services covenants that it will comply with its obligations as a service provider under PIIDPA and will strictly enforce the security arrangements required to protect personal information to which it has access. Symphony Services is also required to confirm the details of those security requirements upon receipt of a request to do so from PNS. PNS employees may at any time travel to the offices of Symphony Services to inspect the security measures it has put in place to protect such personal information.	Canada.

Department	A (Description)	B (Conditions)	C (Reasons)
	2. Check Point Software Technologies Limited provides technical support services to our Firewall environment. There are times when Canadian-based technical support services cannot resolve a technical issue and have to raise the issue with the Check Point's technical head office location in Redwood, California. We would be engaging Check Point's senior technical staff who provide worldwide support of the product. They are based in California, but have support offices in Europe and Israel. In these rare circumstances internal (OCIO) resources allow a PC to be controlled from the external Check Point support resource and the PC screen would be monitored by Government internal resources. A support call may require a Check Point resource login to the firewall to troubleshoot an issue with OCIO staff. This is a rare occurrence, but may occur once every couple of years.	2. The connection to remote control a PC must be initiated by both sides of the connection. Internal support does not leave the terminal while external support is working on the solution. The remote connection does not allow external support to transfer any data remotely. This connection allows internal support the see every step that it takes in order to resolve the problem and/or the option to disconnect the link if and when required. If any system data, not personal data, is required to be sent, it will be sent through a secure encrypted channel.	2. This generic method of external support will: a. Not allow the transfer of personal information over the connection. b. Connectivity will only be enabled upon connection initiation from both sides. No connectivity is automated. It is setup upon a phone call between internal and remote access support and agreement of work to be performed. The connection will not be automatically available for any reason. c. Transfer of any system information will be performed through a secure encrypted methodology. Personal information is not to be sent.
	3. Hewlett-Packard Co. provides technical support services to our	3. The connection to remote control a PC must be initiated by both sides of the	3. This generic method of external support will: a. Not allow the transfer of

Department	A (Description)	B (Conditions)	C (Reasons)
	current operational environment (Hardware Infrastructure and HP Software Suite Openview/Service Manager). There are times when Canadian-based technical support services cannot resolve a technical issue and have to raise the issue with the Hewlett-Packard technical support based locations across the United States. We would be engaging Hewlett-Packard senior technical staff, who provide worldwide support of the product. They are based in the United States (Palo Alto, CA), but have support offices worldwide. In these circumstances OCIO would allow a PC to be controlled by the external Hewlett-Packard support resource and the PC screen would be monitored by OCIO staff.	connection. OCIO Staff do not leave the terminal while Hewlett-Packard is working on the solution. The remote connection does not allow external support to transfer any data remotely. This connection allows internal support the see every step required to resolve the problem and/or the option to disconnect the link if and when required. If any system data, not personal data, is required to be sent, it will be sent through a secure encrypted channel.	personal information over the connection. b.Connectivity will only be enabled upon connection initiation from both sides. No connectivity is automated. It is setup upon a phone call between internal and remote access support and agreement of work to be performed. The connection will not be automatically available for any reason. c.Transfer of any system information will be performed through a secure encrypted methodology. Personal information is not to be sent.
	4. Novell provides technical support services to our current operational environment (file and print sharing, authentication and identity management, server operating system, GroupWise, ZenWorks, etc.). There are times when Canadian-based technical	4. The connection to remote control a PC must be initiated by both sides of the connection. OCIO Staff do not leave the terminal while Novell is working on the solution. The remote connection does not allow external support to transfer any data remotely. This connection allows internal support the see every step	4. This generic method of external support will: a.Not allow the transfer of personal information over the connection. b.Connectivity will only be enabled upon connection initiation from both sides. No connectivity is automated. It is setup upon a phone call between internal and remote access support and agreement of

Department	A (Description)	B (Conditions)	C (Reasons)
	support services cannot resolve a technical issue and have to raise the issue with the Novell's technical support with offices across the United States. We would be engaging Novell's senior technical staff, who provide worldwide support of the product. They are based in the United States, but have support offices worldwide. OCIO would allow a PC to be controlled by the external Novell support and the PC screen would be monitored by OCIO staff.	required to resolve the problem and/or the option to disconnect the link if and when required. If any system data, not personal data, is required to be sent, it will be sent through a secure encrypted channel.	work to be performed. The connection will not be automatically available for any reason. c. Transfer of any system information will be performed through a secure encrypted methodology. Personal information is not to be sent.
	5. Barracuda Networks Inc. provides technical support services to Email Spam Appliances. There may be times when OCIO staff cannot resolve a technical issue and have to raise the issue with the Barracuda technical head office location in Campbell, CA. We would be engaging Barracuda's senior technical staff, who provide worldwide support of the product. They are based in the United States, but have support offices worldwide. In these rare	5. The connection to remote control a PC must be initiated by both sides of the connection. OCIO Staff do not leave the terminal while Barracuda is working on the solution. The remote connection does not allow external support to transfer any data remotely. This connection allows internal support the see every step required to resolve the problem and/or the option to disconnect the link if and when required. If any system data, not personal data, is required to be sent, it will be sent through a secure encrypted channel.	5. This generic method of external support will: a. Not allow the transfer of personal information over the connection. b. Connectivity will only be enabled upon connection initiation from both sides. No connectivity is automated. It is setup upon a phone call between internal and remote access support and agreement of work to be performed. The connection will not be automatically available for any reason. c. Transfer of any system information will be performed through a secure encrypted methodology. Personal information is not to be sent.

Department	A (Description)	B (Conditions)	C (Reasons)
	circumstances OCIO would allow a PC to be controlled by the external Barracuda support resource and the PC screen would be monitored by OCIO staff. 6. Microsoft provides technical support services to our current operational environment (Active Directory, Server Operating Systems, Microsoft SQL Server, etc.). There are times when Canadian-based technical support services cannot resolve a technical issue and have to raise the issue with the Microsoft's technical support based locations across the United States. We would be engaging Microsoft's senior technical staff, who provide worldwide support of the product. They are based in the United States, but have support offices worldwide. In these circumstances OCIO would allow a PC to be controlled by the external Microsoft support resource and the PC screen would be monitored by OCIO staff.	6. The connection to remote control a PC must be initiated by both sides of the connection. OCIO Staff do not leave the terminal while Microsoft is working on the solution. The remote connection does not allow external support to transfer any data remotely. This connection allows internal support the see every step required to resolve the problem and/or the option to disconnect the link if and when required. If any system data, not personal data, is required to be sent, it will be sent through a secure encrypted channel.	6. This generic method of external support will: a. Not allow the transfer of personal information over the connection. b. Connectivity will only be enabled upon connection initiation from both sides. No connectivity is automated. It is setup upon a phone call between internal and remote access support and agreement of work to be performed. The connection will not be automatically available for any reason. c. Transfer of any system information will be performed through a secure encrypted methodology. Personal information is not to be sent.

Department	A (Description)	B (Conditions)	C (Reasons)
	7. IBM provides technical support services to critical hardware infrastructure servers and storage area network equipment. There are times when internal resources cannot resolve a technical issue and have to raise the issue with the IBM's Tier 4 Technical Support who have offices world-wide. In these rare circumstances internal (OCIO) resources allow a PC to be controlled by the external IBM support resource and the PC screen would be monitored by OCIO staff.	7. The connection to remote control a PC must be initiated by both sides of the connection. OCIO support does not leave the terminal while IBM is working on the solution. The remote connection does not allow external support to transfer any data remotely. This connection allows OCIO to see every step required in order to resolve the problem and/or the option to disconnect the link if and when required. If any system data, not personal data, is required to be sent, it will be sent through a secure encrypted channel.	7. This generic method of external support will: a. Not allow the transfer of personal information over the connection. b. Connectivity will only be enabled upon connection initiation from both sides. No connectivity is automated. It is setup upon a phone call between internal and remote access support and agreement of work to be performed. The connection will not be automatically available for any reason. c. Transfer of any system information will be performed through a secure encrypted methodology. Personal information is not to be sent.
	8. Polycom Inc. provides technical support services to Video Conferencing environment, the Bridge and Converged Management Application Appliance. There are times when internal resources cannot resolve a technical issue and have to raise the issue with the Polycom's technical head office location in San Jose, CA. We would be engaging Polycom's senior technical staff, who provide worldwide support of the product.	8. The connection to remote control a PC must be initiated by both sides of the connection. OCIO support does not leave the terminal while Polycom is working on the solution. The remote connection does not allow external support to transfer any data remotely. This connection allows OCIO to see every step required in order to resolve the problem and/or the option to disconnect the link if and when required. If any system data, not personal data, is required to be sent, it will be sent through a secure encrypted channel.	8. This generic method of external support will: a. Not allow the transfer of personal information over the connection. b. Connectivity will only be enabled upon connection initiation from both sides. No connectivity is automated. It is setup upon a phone call between internal and remote access support and agreement of work to be performed. The connection will not be automatically available for any reason. c. Transfer of any system information will be performed through a secure encrypted methodology. Personal information is not to be sent.

Department	A (Description)	B (Conditions)	C (Reasons)
	They are based in the United States, but have support offices worldwide. In these rare circumstances internal (OCIO) resources allow a PC to be controlled by the external Polycom support resource and the PC screen would be monitored by OCIO staff. 9. Cisco Systems Inc. provides technical support services to Layer 2 and Layer 3 Networking Equipment. There are times when Canadian-based technical support services cannot resolve a technical issue and have to raise the issue with the Cisco's technical support based locations across the United States. We would be engaging Cisco's senior technical staff, who provide worldwide support of the product. They are based in the United States, but have support offices worldwide. In these circumstances OCIO would allow a PC to be controlled by the external Cisco support resource and the PC screen would be monitored by OCIO staff.	9. The connection to remote control a PC must be initiated by both sides of the connection. OCIO Staff do not leave the terminal while Cisco is working on the solution. The remote connection does not allow external support to transfer any data remotely. This connection allows internal support the see every step required to resolve the problem and/or the option to disconnect the link if and when required. If any system data, not personal data, is required to be sent, it will be sent through a secure encrypted channel.	9. This generic method of external support will: a. Not allow the transfer of personal information over the connection. b. Connectivity will only be enabled upon connection initiation from both sides. No connectivity is automated. It is setup upon a phone call between internal and remote access support and agreement of work to be performed. The connection will not be automatically available for any reason. c. Transfer of any system information will be performed through a secure encrypted methodology. Personal information is not to be sent.

Department	A (Description)	B (Conditions)	C (Reasons)
Communica-tions NS[2]	Under the Province of Nova Scotia privacy policy, Internet IP (Internet Protocol) addresses are considered personal information. For three Internet-related initiatives," Nova Scotia Come to Life website, Come to Life Pomegranate, and Come to life Canada's University Capital, we used a web statistical analysis service called Google Analytics that involved storing IP addresses on Google's servers in the United States. One employee went to Boston, Dec. 2 - 5 for the annual Christmas tree lighting ceremony. She took a Blackberry and laptop. Both were password protected and necessary for her work dealing with media, event guests, other provincial representatives and to stay in touch with her office in Halifax. Another employee also went to Boston June 2-4 and took his Blackberry so he could check for messages. It was password protected. Two employees from Communications	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.	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. Blackberrys were necessary to make calls, use Twitter and access messages. The laptop was used for writing material and communications.

[2] Note: employees traveling outside of Canada are either traveling for business, or carry their electronic devices to maintain contact with their offices while on vacation.

Department	A (Description)	B (Conditions)	C (Reasons)
	Nova Scotia went to Las Vegas. One from January 22-28 and took her Blackberry. The Blackberry was password protected, and necessary to check for work-related messages. The other employee went from October 14-18. His was also password protected and used for e-mail and to communicate through Twitter.		
Community Services	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 2010 calendar year, three children in care were placed in residential treatment facilities in the US to receive residential treatment services. As part of the referral for placement to a treatment facility, information concerning the child, any medical diagnosis, treatment needs and relevant family information is shared with the placing facility. This information is provided to ensure that the	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.	

Department	A (Description)	B (Conditions)	C (Reasons)
	facility will be able to meet the child's clinical needs and for the purposes 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 the information identified above. The Department of Community Services signed a licensing agreement with the Consortium for Children of San Rafael, California, for the use of a home study methodology known as Structures Family Analysis Evaluation (SAFE). SAFE is copyrighted by the Consortium for Children who own all rights to SAFE. As part of the licensing agreement, the Consortium for Children agreed to perform a yearly audit of files to enable quality control and identify staff training needs. Access to the home studies and supporting questionnaires completed by the	Prior to forwarding the home studies and questionnaires, all identifying personal information was removed by staff of Community Services. Single initials remained to assist in the readability of the home studies. Only individuals assigned to the audit by the Consortium for Children were permitted access to the information from the home studies and questionnaires in order to accomplish the objectives of the audit. The Consortium for Children agreed that the home studies and questionnaires were to be considered confidential and proprietary to Community Services and the Consortium for Children agreed to hold the same in confidence. They have	

Department	A (Description)	B (Conditions)	C (Reasons)
	staff of the Department of Community Services is necessary in order to fulfill the terms of the licensing agreement. A confidentiality agreement was signed with the Consortium for Children outlining the conditions placed on the storage and access of personal information outside Canada.	agreed not to use the confidential information other than for the purposes of the audit to enable quality control and identify refresher needs and to disclose the results only to the Manger of Adoption Services, Department of Community Services. The Consortium for Children agreed to return all copies of the home studies and questionnaires at the completion of the audit by courier and not to use the home studies for further training or demonstration. The Consortium for Children agreed that the home studies and questionnaires would be kept secure at its offices.	
Community Services – NS Housing Development Corporation	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 applicable hardware configuration necessary to operate the application. Tier II application	Under the terms of the contract, Yardi agrees that it will not "use, disseminate or in any way disclosure 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.	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 by the Yardi Systems software operated under an ASP agreement was the best solution. The software provided the best business

Department	A (Description)	B (Conditions)	C (Reasons)
	support is provided by the Yardi Canadian offices operated in Mississauga, Ontario once issues reported are vetted by Housing Authority IT staff. The data is 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.		functionality based on criteria defined at the time of the RFP process for the costs proposed. The technical framework proposed to operate this software was deemed acceptable based on criteria defined at the time of the RFP process for the costs proposed.
Economic and Rural Development and Tourism	N/A	N/A	NS Tourism report included in that of former Department of Tourism, Culture and Heritage, now Communities, Culture and Heritage.

Department	A (Description)	B (Conditions)	C (Reasons)
Education	1. 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). Without an ILS, the libraries could not operate; this service has been identified in the Department of Education's Business Continuity Plan as 'Essential' (Level 3).The ILS contains personal information about identifiable individuals (library clients in Nova Scotia), including name, address, telephone number and email address. This personal information is voluntarily given when a client registers for a library card. Attached to the clients' account number are titles currently on loan to the individual, those for which the individual has been billed and/or has paid, and those which the user has requested.	1. NSPL has implemented reasonable security measures to protect personal and other information in the ILS. The ILS software is maintained on a secure server in Brunswick Place. The contract with the company stipulates that NSPL staff must be contacted when the company requires access to the ILS server. NSPL enables SirsiDynix to access the server for specific upgrade activities at predetermined time periods, at the end of which SirsiDynix staff are logged out by NSPL staff. NSPL staff monitor and audit to ensure the access is reasonable and appropriate. SirsiDynix has no operational requirements to access personal information about clients. Therefore, the risk of access to personal information about Nova Scotians by SirsiDynix is low, but it is technologically possible.	1. The decision was made to continue to with SirsiDynix because there is no Canadian alternative. There are four major ILS vendors in the world who 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. The company serves customers worldwide from its base in the United States.

Department	A (Description)	B (Conditions)	C (Reasons)
	Transaction logs, maintained at NS Provincial Library, 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.		
	2. A number of Department of Education staff traveled outside Canada and had the ability to access personal information contained in email or stored in GroupWise email system, using devices such as the BlackBerry and laptops.	2. Remote access to GroupWise is protected by surname/password authentication and is delivered over an SSL-encrypted link via the secure Blackberry GroupWise server.	2. When staff travel for business reasons (e.g., meetings, conferences), they are expected to monitor their e-mail and voice mail where possible. Therefore, it is necessary for them to check e-mail remotely, where possible, in order to fulfill their responsibilities.
	3. The Provincial Student Information System (SIS) is used by the Nova Scotia education system (schools, school board, Department of Education) to manage school operations, including processes such as student registration and enrolment, attendance, student scheduling, behavior, student	3. 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	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

Department	A (Description)	B (Conditions)	C (Reasons)
	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.	(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 audits 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.	a leading distributor of Student Information System software worldwide.
Energy	**Travel:** Staff traveling outside of Canada may have taken electronic devices including Blackberries and laptop computers which may store and/or access personal information.	**Travel:** Remote access to staff email accounts through web access to GroupWise is protected by username/password authentication and is delivered over an SSL-encrypted link via the secure Blackberry GroupWise server.	**Travel:** When staff travel for work related matters, they may need to carry electronic devices (e.g. Blackberries, laptops) in order to monitor email and/or conduct business for operational purposes.

Department	A (Description)	B (Conditions)	C (Reasons)
Environment	There were two instances where employees traveled outside of the country with their Blackberry's and one of these employees also traveled with their laptop.	No restrictions or conditions were placed on storage or access of the personal information outside of Canada. IAP Office was only notified of the travel after the fact. There would be a very low probability that personal information of Nova Scotians was contained on any of these devices based on the nature of the employees' jobs.	Employees did not access any personal information contained on their devices while out of the country.
Film Nova Scotia	Approximately 3 staff members traveled outside Canada on business. These staff members had the ability to access personal information carried on email or stored in GroupWise via remote access to the GroupWise email system.	N/A	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 - Staff members who traveled outside Canada may have had the ability to access personal information via remote e-mail, Blackberry, or by personal computer. 2. It was necessary for government accounting staff, who are authorized and who were out of the country, to access the	1. Remote access to e-mail is protected by username/password authentication and is delivered over a secure Blackberry GroupWise server. All blackberries must be password protected. TS web access control software is protected by username/password authentication. 2. Access to the SAP system occurred over a secure network connection that prevents other parties from gaining access to the SAP systems. TS web access control software is used in the	1. When staff travel, they are sometimes expected to conduct business or maintain contact with operations. 2. There is a limited number of staff in Government Accounting who are authorized to perform routine and emergency support for the SAP

Department	A (Description)	B (Conditions)	C (Reasons)
	provincial SAP systems (Financials) via a secure remote network connection in order to provide routine and emergency support.	Provincial Government to ensure the protection of personal information while being accessed remotely. Access is restricted and controlled by the Province and no transaction to SAP systems is permitted without the knowledge and approval of Division management.	(Financials) system. Remote access services are required to meet the mandate of the Government Accounting Division in the performance of services to numerous departments.
	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 several times throughout the reporting period as required to	3. When SAP Support Staff have reason to access any of the Province's SAP systems as a part of problem remediation, all production system transaction access is approved by CIS Division management and all access activity is recorded in an audit log so that verification can be done of whether personal information has been accessed. In addition, this access occurs over secure network connections that must be opened to allow SAP to enter a specific system. This secure network connection also prevents other parties from gaining unauthorized access to the SAP systems. This type of remote access very rarely involves actual access to personal information and is typically limited to system operations information. In cases where approved access does involve potential access to personal information	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)
	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.	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.	
Halifax Dartmouth Bridge Commission	The Halifax Dartmouth Bridge Commission's (HDBC) MACPASS software application maintenance and support is provided by VESystems primarily located in Irvine California. VESystems provide both routine maintenance and upgrades, and thus have access to personal information through a portal to HHB's internal network. Access is fairly routine and would occur minimally once a month.	The access is controlled though 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 HHB and its ability to conduct and operate its electronic toll collection program. The system was purchased in 2008 and has been maintained by its developer, VESystems, since implementation.
Halifax Regional Water Commission	Halifax Water authorized 52 staff members to transport personal information devices such as laptop computers, cell phones and electronic data storage devices outside of Canada.	These devices were taken by staff to ensure they remained in contact with other utility staff to fulfill operational responsibilities.	Halifax Water owns and operates water, wastewater and storm water systems which are deemed critical infrastructure by the Government of Canada.

Department	A (Description)	B (Conditions)	C (Reasons)
Health and Wellness	1. **Storage:** There were no approvals granted for the storage of personal information in the custody or control of the Department of Health outside of Canada from January 1, 2010 – December 31, 2010. 2. **Access:** The Department of Health granted the following approvals for access to personal information in the custody or control of the Department of Health outside of Canada from January 1, 2010 – December 31, 2010: a. **McKesson Corporation, STAR Patient Processing:** The McKesson STAR Patient Processing system is the patient admission tool currently implemented in the CHDA. 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,	a. **McKesson Corporation, STAR Patient Processing:** McKesson developers need to access the local provincial Client Registry from their offices, outside of Canada to deploy the software changes and test the enhanced software with the provincial Client Registry. The client Registry data will not be stored outside of the country. McKesson's development staff will use a pre-existing secure 'data tunnel' to connect the McKesson test system to the provincial Client Registry test system to	a. **McKesson Corporation, STAR Patient Processing:** McKesson will be enhancing CDHA's patient admission tool to support the provincial Electronic Health Record's (HER or SHARE's (Secure Health Record) integration requirement for patient active admissions, discharges and transfers. The McKesson product used to register patients in CDHA is proprietary to McKesson so no other vendor can perform the changes. The McKesson code and product development site is located in the United

Department	A (Description)	B (Conditions)	C (Reasons)
	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.	complete the enhancement testing. The provincial Client Registry is located in the HITS-NS data center. All users accessing the data will require security sign-on to the Star-Patient Processing system and will need to be given access to the provincial Client Registry integration by the hospital IT staff. Select McKesson developers/testers will have access to the test system. McKesson developers/testers will be pre-approved and must sign a confidentiality agreement. McKesson developer's/testers access will be terminated immediately at test completion which is forecast for April 30, 2010. No personal information will be downloaded or copied by McKesson. All requests into the registry will be tracked and audit reports provided for review. McKesson Corporation is committed to following all Health Insurance Portability and Accountability Act ("HIPAA") regulations and all Ministry requirements for protecting patient information in Canada. HIPAA is United States federal law which includes provisions of the protection of privacy of certain	States.

Department	A (Description)	B (Conditions)	C (Reasons)
		individually identifiable health information referred to as protected health information.	
	b. **FairWarning:** FairWarning is an appliance based application that facilitates the creation of privacy audit reports for health information systems. The FairWarning tool allows audits to be conducted of user access to electronic health information systems. FairWarning staff require access from outside of Canada to assist in the set up and ongoing maintenance of the FairWarning application; this includes having access to the application audit log database that contains limited personal information. FairWarning may also assist in providing FairWarning application training to District Health Authority Privacy Leads and other appropriate DHA/Department of Health/HITS-NS staff using the application and audit log data.	b. **FairWarning:** The Master Agreement with FairWarning prohibits storage or access of personal information outside of Canada unless the Department of Health consents in writing. FairWarning's development staff will use a pre-existing secure 'data tunnel' (VPN) to connect to the information stored on the appliance server to complete the configuration and testing of reports. The appliance server is located in the provincial data centre. Select FairWarning project managers/developers/testers will have access to 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	b. **FairWarning:** The FairWarning application will be used to augment current user access audit approaches for various provincial health information systems. FairWarning is an appliance based application that facilitates the creation of privacy audit reports for health information systems. The FairWarning tool allows audits to be conducted of user access to electronic health information systems. The application will be used to augment current user access audit approaches for various provincial health information systems.

Department	A (Description)	B (Conditions)	C (Reasons)
		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.	
	3. **DOH Employee Access:** Between January 1, 2010 to December 31, 2010 twenty-seven staff of the Department of Health traveled outside Canada and has the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise system.	3. **DOH Employee Access:** The Department of Health *Transmission of Confidential Information by E-mail and Fax* guideline (2004) prohibits the inclusion of personal information in e-mail sent outside the GroupWise system unless the e-mail is encrypted and password protected. The Guideline also recommends limiting the inclusion of personal information contained in e-mail within the GroupWise system. Therefore, the amount of personal information held or sent by e-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.	3. **DOH Employee Access:** 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 for them to check e-mail remotely where possible in order to fulfill their responsibilities.

Department	A (Description)	B (Conditions)	C (Reasons)
In*NOVA*Corp	There were 8 individuals who traveled for business or pleasure, and through those 8, there were 19 different acts of access, which included VPN access, blackberry access and/or webmail. Access was within North American and included Arizona, California, Chicago, Florida, Maine, Massachusetts and Washington. In addition, In*NOVA*Corp uses the following during the normal course of business.- IBM (formerly American Express) Online expense reporting - dates are Jan 01, 2010-Dec 31, 2010- Facebook and Twitter for social marketing purposes - dates are Jan 01-Dec 31, 2010- WebEx and Skype for web conferencing purposes - dates are Jan 01-Dec 31, 2010- SurveyMonkey is used for employee survey purposes - dates are March 1-August 30, 2010- Slimtimer for on-line time tracking purposes - dates are Jan 01-Dec 31, 2010.	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 and are 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 a reasonable and direct connection to the person's job duties while traveling outside Canada.
Intergovern-mental Affairs	In 2010, Intergovernmental Affairs continued to use Iron Mountain's services for records	The service contract with Iron Mountain states: 1. Iron Mountain is to contact	This decision was made to address the issue that the department has limited space while at the same time business

Department	A (Description)	B (Conditions)	C (Reasons)
	storage. In 2006, we 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 according to the STOR retention schedule were not eligible 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 upon the receipt of a subpoena or similar order unless such notice is prohibited by law. 2. Confidential Information shall be held in confidence by Iron Mountain and shall be used only in the manner contemplated by the agreement. 3. 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.	activities create records that remain relevant for long periods of time. Iron Mountain specifically was chosen, because at the time no Canadian owned competitor in Nova Scotia could be found. Furthermore they are considered to be the industry lead. In the past year, Intergovernmental Affairs has made every effort to reduce its holdings at Iron Mountain. With a new STOR in place, Intergovernmental Affairs has removed 38% of the total records stored at Iron Mountain, having transferred them to the Government Records Centre or Provincial Archives. Additionally when selecting our new office location records needs were better factored into the design and active records will once again be held at the department. Intergovernmental Affairs plans to terminate its relationship with Iron Mountain by the end of the first quarter of the fiscal year 2011-2012.
Justice	1. In Legal Services, the litigation lawyers and administrative staff use a document management program called Practice Manager to store all case material. While the database is stored on DOJ servers, from time to time when there is an issue with the program,	Information is stored or accessed outside of Canada in compliance with contract.	

Department	A (Description)	B (Conditions)	C (Reasons)
	DOJ contacts the provider Automon, which is a US company, and to resolve the issue they conduct a live meeting in order to access the computer and program to see what's going on. 2. DOJ has approximately 16,000 records stored with Iron Mountain. They are located at the Blue Water Acres facility but are an American owned company. Senior staff toured the facility in connection with privacy issues quite some time ago. 3. In accordance with the Hague Convention on the Civil Aspects of International Child Abduction, the Department of Justice acts as the Central Authority for Nova Scotia. A DOJ Lawyer represents the Central Authority for Nova Scotia in this regard. The role of the Central Authority involves forwarding applications and information about the parents and children to the Central Authority in member states to which children have been taken or in which they are being retained. The Central		

Department	A (Description)	B (Conditions)	C (Reasons)
	Authority for Nova Scotia also facilitates applications commenced in Nova Scotia by left-behind parents in member states. In both incoming and outgoing cases, certain relevant personal information of the parents and children flows through the Nova Scotia Central Authority to member states in accordance with the requirements of the Convention. 4. Staff members who traveled outside Canada on business may have had the ability to access personal information via remote e-mail, Blackberry, personal computer or by any other means. 5. Staff members who traveled outside Canada on pleasure may have had the ability to access personal information carried on e-mail or stored on GroupWise via remote access to GroupWise email system.	4. Remote access to Group Wise is protected by username/password authentication, and is delivered over and SSL-encrypted link via the secure Blackberry GroupWise server. 5. Remote access to GroupWise is protected by username/password authentication, and is delivered over and SSL-encrypted link.	4. When staff is travelling for business reasons they are expected to monitor their email and voicemail for business continuity purposes. 5. When staff is traveling for pleasure they may be required to maintain contact with operations.
Labour and Workforce Development	1. NS Labour &Workforce Development utilizes NRSPro.com (formerly GEDScoring.com) software for	1. The department has a contract with NRSPro which stipulates that all information will be kept private and confidential and will not be released to	1. The department completed an evaluation of options for delivery of the Nova Scotia GED program in November of 2001. It was determined that there

Department	A (Description)	B (Conditions)	C (Reasons)
	the purpose of storing and processing information, in support of the General Educational Development (GED) program. 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	any third party unless authorized by the department in writing. The contract also states that only personnel authorized by the department will be provided access to store and retrieve Nova Scotia information. The transmission is over a SSL connection using an encrypted link. The test results and certificates are also available for viewing by authorized LWD staff on the NRSPro web site, using the same security methods. A user ID and password are also required for access. The department scans the test sheets locally and sends data to NRSPro over an encrypted Secure Sockets Layer (SSL) connection. The information is stored in a database at NRSPro located in Spanish Fork, Utah, USA, for processing and as a record for future reference. Continued storage is required for data retrieval and combining of score results for students 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.	were only two vendors (OSS & NRSPro) certified by GEDTS to conduct test scoring that the department felt confident would be able to handle Canadian requirements. Both vendors were application service providers (ASPs) 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,

Department	A (Description)	B (Conditions)	C (Reasons)
	Scotia. The department scans the test sheets locally and sends data to NRSPro over an encrypted Secure Sockets Layer (SSL) connection. The information is stored in a database at NRSPro located in Spanish Fork, Utah, USA, for processing and as a record for future reference. Continued storage is required for data retrieval and combining of score results for students re-writing tests that were not passed successfully. The test scoring is completed remotely by NRSPro and the test results and certificates are transmitted to the department in PDF files for printing locally. The information is transferred by NRSPro to the General Educational Development Testing Services (GEDTS) international database. The international database contains information used for statistical reporting of GED achievements by jurisdiction. This includes gender, age, country, province, number of participants, number passed, number failed, etc. GEDTS is located in Washington D.C., the		OSS came highly recommended by GEDTS. n July, 2009 the department terminated our contract with OSS and began working with NRSPro.com. Data was transferred to our new service provider, NRSPro. NRSPro had been the department's scoring service provider from 1993 to 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)
	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. 2. There were 8 employees who traveled outside Canada with a Blackberry device, with some contact information, and may have accessed personal information through email.		
Natural Resources	1. There was no storage of personal information in the custody or control of the Department of Natural Resources outside of Canada from January 1, 2010 to December 31, 2010. 2. Staff members who traveled outside Canada on business may	2. Remote access to Group Wise is protected by username / password authentication, and is delivered over an	2. When staff are traveling for business reasons they are expected to monitor their email and voice mail for business

Department	A (Description)	B (Conditions)	C (Reasons)
	have had the ability to access personal information via remote e-mail, Blackberry, personal computer or by any other means. 3. 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 via remote access to GroupWise email system. 4. Off site record storage contracted with Iron Mountain Canada (subsidiary of the American Company)	SSL-encrypted link via the secure Blackberry GroupWise server. 3. Remote access to Group Wise is protected by username / password authentication, and is delivered over an SSL-encrypted link 4. Iron Mountain is to safeguard and maintain protected storage of the Departments Records. Iron Mountain Canada Corporation confirms that personal information is maintained and disclosed in accordance with our contractual arrangement in compliance with all applicable privacy legislation.	continuity purposes. 3. When staff is traveling for pleasure they may be required to maintain contact with operations. 4. Off site storage of backup media/microfilm is required as part of the Disaster Recovery Program. The offsite storage is required to ensure recovery of 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	**1. salesforce.com inc – CRM data services – storage and access – individuals' business contact information** The individuals' business contact information is to be protected in accordance with the sales.force.com inc master agreement and privacy statement which recognize NSBI as owner of the	**1. salesforce.com inc – CRM data services – storage and access – individuals' 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

Department	A (Description)	B (Conditions)	C (Reasons)
	information in NSBI's custody/control, as part of customer relationship management (CRM) data services supplied under contract by salesforce.com inc (a Delaware, US corporation with its principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.	stored data and provide strong privacy protection and security processes. The service is certified as a "Safe Harbour" under the EU Directive on Data Privacy and is certified "TRUSTe" privacy compliant.	Salesforce® data service was selected through independent evaluation and based on its superior standing in meeting predefined objective evaluation criteria (including service functionality, IT compatibility, data security, vendor experience and cost). The tangible risk of compromising these critical service requirements outweighs the remote risk of business contact information (given its more accessible public nature) being the target of a foreign demand for disclosure.
	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	**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 as 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.

Department	A (Description)	B (Conditions)	C (Reasons)
	place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation. **3. International In-market consultants – trade development & investment attraction services – storage and access – personal information (primarily business contact information)** Pursuant to s. 5(2) *PIIDPA* the head of NSBI determined the storage/ access outside Canada of personal information (primarily business contact information) in NSBI's custody / control, as part of the investment attraction and trade development services supplied under contract by international in-market consultants (global) is to meet the necessary requirements of NSBI's operation. **4. NSBI directors, officers, employees – performance of duties during international travel – storage and access – personal information**	**3. International In-market consultants – trade development & investment attraction services – storage and access – personal information (primarily business contact information)** The personal information (primarily business contact information) is to be protected in accordance with the service agreement including confidentiality provisions. **4. NSBI directors, officers, employees – performance of duties during international travel – storage and access – personal information**	**3. International In-market consultants – trade development & investment attraction services – storage and access – personal information (primarily business contact information)** NSBI engages international in-market consultants as an essential and integral component of NSBI's trade development and investment attraction activities. The consultants are experts in the business environment within a business sector or geographic region of interest. International consultants operate from and travel outside Canada and must be able to store and access personal information (primarily business contact information) outside Canada in order to facilitate business connections / transactions in performing their contracted services. **4. NSBI directors, officers, employees – performance of duties during international travel – storage and access – personal information**

Department	A (Description)	B (Conditions)	C (Reasons)
	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.	Personal information stored in or accessed during 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, office or employee in accordance with the NSBI Code of Conduct and Oath of Office and the NSBI Privacy Policy.	For business continuity purposes, NSBI directors, officers, employees must be able to store and access, using a mobile electronic device, personal information that has a reasonable and direct connection to the person's job duties so the person can perform work responsibilities while traveling outside Canada.
Nova Scotia Liquor Corporation	1. **Storage:** There is storage of NSLC employee work hours and times in the U.S. to allow chosen service provider ADP to perform payroll functions on our behalf. 2. **Travel:** There was access to personal information using wireless data devices including Blackberrys and laptops on a daily basis while employees were working outside Canada.	1. **Storage:** This was declared in a letter two years ago and nothing has changed since that time. 2. **Travel:** The conditions placed on such access involved the use of encryption via VPN technology and password protection.	1. **Storage:** Our preferred payroll provider ADP does not provide time and attendance processing calculations where the data is stored only in Canada. Other service providers did not offer an adequate solution. 2. **Travel:** Such access is granted to allow employees to perform some of their duties while absent from their offices.
Public Prosecution Service	1. There was no storage of personal information outside Canada by the Public Prosecution Service in 2010.		

Department	A (Description)	B (Conditions)	C (Reasons)
	2. There was access to personal information using wireless data devices, including Blackberries and laptops on a daily basis while staff visited countries outside Canada (Note: employees traveling outside of Canada are either traveling for business, or carry their electronic devices to maintain contact with their offices while on vacation) at the following locations: Czech Republic, The Netherlands, United Kingdom, Bermuda, Vermont, Maine, New Hampshire, Maui, New York, Florida, The Bahamas, Cayman Islands, Honduras, Mexico, Boston, Buffalo.	2. The conditions placed on access involved the use of encryption and password protection.	2. Access was granted in order to permit staff to discharge some of their responsibilities while absent from their offices.
Service Nova Scotia and Municipal Relations	1. In 2006, L-1 Identity Solutions (formerly Digimarc) of Billerica, Massachusetts, was awarded a contract to provide Photo License/Photo ID equipment, software integration, and support services to the Registry of Motor Vehicles. This contract included a major upgrade to the Photo License/ID Card system in 2010.	1. Access from the Billerica and Fort Wayne locations is restricted via VPN username/password and on the image/database server by the privileged account username/password. Access will be in response to escalated support calls only.	1. Access by L-1 Identity Solutions personnel in Billerica and Fort Wayne is an operational requirement in response to Photo License/Photo ID system outages that affect the delivery of customer service.

Department	A (Description)	B (Conditions)	C (Reasons)
	The Photo License image/database server (a key component of the system which stores client photos, digitized signatures, personal information, and Driver Master Number) is located at the Provincial Data Center in Halifax, Nova Scotia. In 2006, Digimarc support technicians in Billerica, Massachusetts and Fort Wayne, Indiana were provided remote access via VPN to the image/database server in order to provide tier II/III support. Routine maintenance and support for this system is provided by Halifax-based L-1 field technicians, with the Billerica and Fort Wayne technicians acting as back-up personnel and/or handling escalated problems that the local technicians are unable to resolve.		
	2. The Interprovincial Record Exchange 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	2. CCMTA acts as the clearing house for all queries so that jurisdictions do not have direct read access to another jurisdiction's system. Queries are forwarded to/from member jurisdictions only (CCMTA & AAMVA). Queries are pre-formatted and specific as to what information is displayed. CCMTA has	2. Promotion of road safety and law enforcement so that a driver's license or vehicle permit may not be fraudulently transferred from one jurisdiction to another, and infractions occurring in another jurisdiction are recorded on the driver's record in Nova Scotia.

Department	A (Description)	B (Conditions)	C (Reasons)
	the clearing house and administrators for this system, and operates the secure network over which it runs. A partnership arrangement now exists with the American Association of Motor Vehicle Administrators (AAMVA) to extend the system to the US.	contracts with each of its member jurisdictions that conform to the jurisdiction's privacy legislation concerning disclosure and consent.	
	3. Credit card transaction information resulting from payments for on-line services through ACOL or SNSMR, in-person services at Access Centers, Land Registration Offices, and the Business Registration Unit, or mail-in services is subject to transborder data flow through US-based credit card processing services for payment authorization and account reconciliation. Personal information that is transmitted through or stored in the US is at risk of a foreign demand for disclosure under the Patriot Act.	3. All service providers in the credit card payment chain are subject to strict security precautions to protect credit card information from unauthorized or accidental disclosure. The service providers are Payment Card Industry - Data Security Standards (PCI-DSS) certified, and must also follow terms and conditions as defined by the card issuing institutions. Cardholders have agreed to the card issuing institutions' privacy statements that include a notice that third-party service providers may be used to process credit card transactions.	3. SNSMR offers credit card payments as a convenience for customers, and to provide efficient and effective on-line services to clients.
	4. Twenty-three (23) SNSMR staff traveled outside Canada during the reporting period and accessed GroupWise email from a	4. Remote access to GroupWise is protected by Username/Password authentication, and is delivered over an	4. Maintain contact with operations.

Department	A (Description)	B (Conditions)	C (Reasons)
	laptop or Blackberry while away.	SSL-encrypted link.	
Trade Centre Limited	The ticketing system used by Ticket Atlantic is hosted in Irvine California, USA by Paciolan. The data is housed in their managed facility on their AS6000 mainframe computers. Secure access is provided from TCL facilities to the data centre via a secured VPN tunnel. This is data required for the sale and purchase of event tickets from Ticket Atlantic Box Office and is under the ownership of TCL.	Only Ticket Atlantic employees and agents can access the information through the secured VPN tunnel. Our contract states that Paciolan will only use the collected customer information solely for the purposes contemplated in this agreement and otherwise in compliance with all applicable federal and state laws. (the) Customer will own all Personal Information, data and related information collected or received through use of the System by it, or directly by Paciolan, and all compilations thereof, in connection with the operation of the system. Data is stored to ensure we can reconcile delivery of tickets, returns, discrepancies and payment verification to the customer. Customers are asked if they wish to receive future information on events, etc. and only then will they be sent any correspondence outside the ticket purchase for which the information was supplied. 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	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 model - the system is not available to be installed on premises. 5 year contract was extended for 2 years. We are in year 1 of the 2 year extension. 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.

Department	A (Description)	B (Conditions)	C (Reasons)
		account.	
Transportation and Infrastructure Renewal	Ten employees were granted approval to use cell phones, Blackberry's or laptops while traveling outside Canada to allow contact with co-workers should any questions arise and to deal with matters of urgent issues, etc.	Access to GroupWise system was protected by username/password authentication which is delivered over SLL/encryption.	Blackberry use is protected by username/ password authentication which is delivered over SLL link/encryption. As well, employee to comply with PIIDPA Section 5 & 9(4) and the recommendations provided by the Chief Information Officer regarding safe and secure transport and storage of portable storage devices.
Utility and Review Board	Payroll details of Board Members and staff were held by Ceridian Canada Inc., a payroll service provider operating in Canada but owned by a parent company resident in the United States.	Data were required to be held as confidential records by the payroll service provider. Information was stored on servers located inside Canada.	Ceridian is a longstanding payroll provider for the Board. A Canadian service provider was sought but none were found suitable.
Worker's Compensation Board	**Travel:** 20 instances of staff traveling with smartphones (Blackberries or iPhone). Access to personal information through a secure portal into the WCB's internal network.	Immediate report of theft/loss of information.	Out of Country travel request to be prepared by staff and management, approved by the CEO/Vice President/Chair prior to travel. The CEO/Vice President may provide direction on any appropriate restrictions to ensure we are protecting the personally identifying information of our customers.

Table 2: January 1 – December 31, 2010 Foreign Access and Storage by Health Authorities

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Annapolis Valley District Health Authority (AVDHA)	**1. CONTRACTS:** AVDHA entered into 44 service contracts. These contracts were reviewed to identify if any contracts allowed or required storage or access of personal information outside of Canada. None of these contracts allow/require storage or access of personal information outside of Canada. **2. TRAVEL:** It is our estimation that 12 AVDHA employees traveled outside of Canada and may have accessed personal information via laptop, Blackberry or PDA's.	1. All new and renewed contracts have will have inclusion clauses added to contracts requiring vendors to comply with PIIDPA legislation. Privacy Impact Analysis must be completed on all new systems. E-courier is used for emailing personal information outside of the NSHEALTH network. 2. All laptops, Blackberry devices, PDA's are password protected. Laptops and removable USB storage devices (flashdrives) are encrypted. Blackberry devices also have an auto-wipe feature.	1. Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized in the AVDHA and are deemed necessary in the operations of these systems and programs.
Cape Breton District Health Authority (CBDHA)	**1. Travel** - Approximately 5 employees traveled outside of Canada and may have accessed personal information via remote e-mail or Blackberry.		

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	2. <u>Contracts</u> – 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, 3M for HDM system and NRS Module; 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 and Pegasys Ultra.	**2. <u>Contracts</u>** - All new and renewed contracts have inclusion clauses requiring vendors to comply with PIIDPA legislation.	**2. <u>Contracts</u>** – Current access to 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.

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
Capital District Health Authority (CDHA)	A decision was made to permit certain product vendors to potentially access personal information outside of Canada where required for the repair or maintenance of equipment and information technology systems required for the operations of the health authority where the required expertise were not available within the health authority.	All new and renewed contracts involving the potential for storage or access of personal information outside of Canada have inclusion clauses added to contracts requiring vendors to comply with PIIDPA legislation. In addition, CDHA general information and sharing policies apply in this situation including its Privacy Policy.	Current access to and storage of information outside of Canada is linked to pre-existing programs and/or systems utilized in CDHA and deemed necessary for operations.
Colchester East Hants Health Authority (CEHHA)	1. **Access by Staff:** For the period January 1, 2010 - December 31, 2010, approximately 5 employees travelled outside of Canada and may have accessed personal information via remote e-mail, Blackberry or Treo's. 2. **Contracts:** No contracts were renewed or signed during this reporting period.	Guidelines will be developed related to access/storage of personal information outside of Canada.	Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized in the Colchester East Hants Health Authority and are deemed necessary in the ongoing operations of these systems and programs. Specific CEHHA guidelines related to reporting on decisions on access and storage of information from outside of Canada will be developed.
Cumberland Health Authority (CHA)	Decision made to provide the following (including but not limited to):	Access to information stored on CHA networks and servers is only permitted	Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized in the

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	1. VPN access to Dictaphone System from Florida, US offices for remote vendor application support. 2. Encrypted (SSL) staff access to CHA web mail system from US locations. 3. Storage of information on whole disk encrypted DHA owned laptops. 4. Access to email using Blackberry mobile devices.	through encrypted VPN connections. All external email access is encrypted through SSL, VPN (IPSEC) or the Blackberry service. The CHA had 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. 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. Guidelines will be developed	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)
		related to access and storage of personal information outside of Canada.	
Guysborough Antigonish Strait Health Authority	Blackberry usage outside of Canada- Facility Manager Guysborough Memorial Hospital from February 17-20, 2010 (Pittsfield, Maine). CEO took his blackberry to Miami from April 8-17, 2010.	None None	Individual notified the IT Director who keeps inventory of travel outside of Canada with electronic devices. CEO notified Director of IT that he would be travelling outside of Canada. She compiles list for end of year PIIDPA submission.
IWK Health Centre	For the 2010 calendar year, IWK's records indicate 154 business/work-related trips were made outside of Canada, as reported by the various cost-centres funding the travel. This number represents the number of trips booked through IWK for travel outside of Canada, and does not necessarily equate to the number of potential accesses to personal information. The 154 trips outside of Canada were made by 120 different individuals. When individuals travel with laptop computers and/or other mobile electronic devices (such as	Employees of IWK who travel outside of Canada do not take personal information with them, but from time to time, may access personal information through laptop computers or other mobile electronic devices (blackberries, iPhones, etc). A formal policy is being developed by the privacy leads of the various provincial District Health Authorities/IWK for the purpose of delineating	

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	blackberries, iPhones, etc.), generally the devices are used to gain access to email accounts only, and direct access to health centre files (which may contain personal information) is not advised or supported. While remote access to other IWK information systems which contain personal information is possible, laptops have encryption software to protect information accessed with/stored on them, all handheld devices are password protected to protect information stored on them, and remote access via protected terminal services/remote desktop sessions is encouraged. IWK contracts with certain service providers located outside Canada for specialized services. The services provided by these vendors are considered necessary for the requirements of IWK's operations, and can require vendors to have remote access to IWK systems potentially resulting in access to, or storage of, personal information outside Canada. Standard remote access for vendors is controlled by IWK's Privacy Office and	conditions and restrictions for access to personal information by employees who travel outside of Canada. At present, IWK has implemented various restrictions and conditions to safeguard personal information in the context of employee travel outside of Canada: Employees are advised how to configure their handheld devices during travel outside of Canada so that email is 'turned off' (not accessible) if not required, while still allowing the telephone part of the device to be accessible. All IWK blackberries are password protected, and the mandatory use of passwords is enforced. As an additional precaution, if a user fails to enter the correct password within a limited number of attempts, the device automatically 'wipes' itself clean of all content. The ability to remotely 'wipe' the content of	

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	specific IWK protocols requiring completion of remote access forms. This access is facilitated by IWK's IT department and HITS Nova Scotia, who assist in the installation of specific VPN software on services providers' systems. For very large vendors who have the infrastructure to support it, Site to Site VPN access is permitted and terms of access are contractually controlled. Before entering into contracts with these service providers, contracts are reviewed and contractual conditions are included wherever appropriate such as confidentiality clauses, secure network access requirements and other accountability provisions and processes to safeguard personal information. IWK contracts with laboratories outside Canada for the provision of certain specialized laboratory testing services which are either not offered in Canada, or the cost of which if provided in Canada is prohibitive. Consent is obtained from patients when circumstances allow and IWK Laboratory Services carefully tracks all external laboratory referrals, both	the devices has also been configured. As an additional protection measure, iPhone support has been enabled against IWK's Exchange Servers (e-mail, contacts, calendars and tasks natively using Exchange Active Sync component), and a set of minimum standards have been implemented to ensure only iPhone devices that support hardware encryption are allowed to integrate IWK's server. The 'remote wipe' and 'limited password attempt' safeguards have also been implemented with respect to IWK employee/physician iPhones. With respect to laptop computers, all newly introduced IWK laptops have been updated with encryption software to safeguard all information stored on/located on any lost, stolen or improperly accessed laptops, including USB portable memory drives used in the laptops, in the event	

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	inside and outside of Canada.	unauthorized user attempts to gain access. IWK's remote access practices and policies clearly identify for employees and physicians that direct access to health centre files is not a supported method of accessing information. Rather, where possible, employees and physicians are granted access to Terminal Servers and/or Remote Desktop Sessions, which connects them directly to their work computers at the health centre. Care has been taken to deploy 'Active Directory' software protections to these Terminal Servers and Remote Desktop Stations, which essentially allows IWK network administrators to control what users are able and not able to do remotely when accessing the IWK network and systems, including the prevention of copy/paste, remote printing and mapping of serial and printer ports.	

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		This has all been done so that remote access solutions are 'windows' into IWK's systems, without allowing information to be taken offsite. When personal information has the potential to be accessed from outside of Canada or be stored outside of Canada by service providers or partners, the IWK either obtains the individuals consents' for such storage/access to their personal information outside of Canada, or uses contractual conditions pertaining to confidentiality and protection of confidential information to restrict/control the service provider's processes for access/storage of the information. Additionally, the IWK Privacy Officer undertakes a 'Privacy Impact Assessment' (PIA) if a new service is implemented at the health	

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		centre which involves or requires the transmission, storage or potential access of personal information by partners or service providers located outside of Canada, or if they are subsidiaries of parent companies located in the United States. The PIA is reviewed by the Privacy Officer to ensure that risks of disclosure of personal information are properly addressed and mitigated. With respect to research conducted at the IWK where the 'sponsor' is located outside of Canada, no personal information is shared or provided to the sponsor before and until consent to do so has been obtained from the patient (or patient's legal guardian). 'Survey Monkey' is a web-based surveying tool used by IWK. Because the server for 'Survey Monkey' is located outside of Canada, and therefore so is the data,	

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
		access to this tool is restricted on IWK's network. The restricted access was implemented and the reasons for it communicated to IWK employees and physicians on May 1, 2009. Access remains restricted to-date and authorization from the head of IWK is required to access this tool on the network.	
Pictou County Health Authority (PCHA)	Access and storage from outside Canada is linked to pre-existing programmes and/or systems utilized at PCHA which continue to be required to be used for the necessity in ongoing operation of these systems and programmes (e.g., Meditech, Dictaphone, 3M). PCHA Senior Leaders may have accessed personal information while conducting business outside the country using remote e-mail and Blackberry.	Vendors are required to follow PIIDPA legislation. Staff is required to follow PCHA's privacy policies.	Access and storage from outside Canada is linked to pre-existing programmes and/or systems utilized at PCHA which are required for ongoing operations of these systems and programmes.
South Shore Health Authority (SSHA)	1. South Shore Health has an agreement with manufacturer Phillips Respironics for two Sleepware Systems, which allows access to our computer network from the company's	1. and 2. The following clause appears in all requests for proposals and Tenders award by the SSHA: Vendor acknowledges that in the	1. Current storage and access to information from outside Canada is linked to pre-existing programs/ software used within South Shore Health and is deemed necessary for

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	service helpline located in the United States. 2. South Shore Health purchased cardiac monitors from SpaceLabs. The software for this company allows its head office in the United States to access computer servers within SSHA containing patient names and hear patterns for maintenance and repairs.	performance of any Contract awarded hereunder it may obtain information concerning individuals which information is subject to protection in accordance with applicable legislation and regulation including, without limiting the generality of the foregoing, the Personal Information International Disclosure Protection Act ('PIIDPA') and any other applicable Act or regulation. Vendor agrees to safeguard any such information in accordance with all such legislation/regulation and use same solely to comply with its obligations under the awarded Contract.	continued operations, in this case, to ensure ongoing patient care. 2. This access to information from outside Canada has been deemed necessary to support ongoing clinical investigations and patient care.
South West Nova District Health Authority (SWNDHA)	In 2010, 16 SWH employees were involved in international travel where they may have maintained access to the organization through cell/blackberries, remotely through VPN or through the nshealth.ca web network. The countries involved are the USA (Chicago), Jamaica, Mexico and	The district continues to add the inclusion clause re: the management of information in all requests for proposals, new contracts, warranties or renewals.	SWH uses software vendors located outside Canada who maintain system remotely, for example, Meditech (health information); SAP (financial and personnel); Nuance (Transcription/dictation); Siemens (DI equipment). Again, the access to systems are managed by written

District Health Authority	A (Description)	B (Conditions)	C (Reasons)
	Kuwait. SWH implemented SAP in April, 2009. This provincial program did undergo a Privacy Impact Assessment and change since 2010 relating to access were reviewed by DHA privacy. COGS (Centre of Geographical Science) software used to evaluate service information and create care maps for program. SWH entered into 3 application maintenance contract with the following vendors: Readiometer, Siemens, Somagen Diagnostics.		agreements and monitored by SWH.

Table 3[3]: January 1 - December 31, 2010 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.	1. Access is restricted to authorized technical support carried out by working with a CBU employee, possibly on-line. Access to this information is authorized for the purpose of required assigned duties and research.	1. 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:** Faculty may access portions of the CBU Student Information System when out of the	2. Access to student records is permitted to those employees in positions requiring access to fulfill their job requirements at the university and is managed through authorized user	2. The system is required to meet the operational requirements of the university.

[3] Acadia University, University of King's College and Université Sainte-Anne reported that they had no foreign access or retention of personal information outside of Canada.

Universities	A (Description)	B (Conditions)	C (Reasons)
	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. Students have web access to the student information system to view their individual financial and academic records. 3. **Course Management System:** CBU uses MOODLE as its course management system. The system facilitates on-line learning for both on-campus students and those studying from a distance. Web access is available to this system for both faculty delivering courses and students	accounts. Student access is limited to viewing their own record information and is managed through authorized student accounts. 3. Access to MOODLE is restricted to those faculty delivering and students registered in CBU courses during a particular term. The data accessed is restricted to course materials.	3. The system is required to meet the operational requirements of the university.

Universities	A (Description)	B (Conditions)	C (Reasons)
	enrolled in the courses. 4. **Travel:** Approximately 38 staff members traveled outside of Canada with web access to their personal email via smart phone 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.	4. Web access to travelling employees is restricted to email and is available to authentication users only.	4. Remote access to email is required by employees to meet the operational requirements of their positions.
Dalhousie University	1. **Financial Services.** Service provider for the creation of templates for various electronic financial services, e.g. purchase orders, bills, cheques, etc.	1. **Financial Services.** Limited access: only where required for maintenance and troubleshooting. Personal information stored internally. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie	1. **Financial Services.** This is the only product offered which offers integration with the University's well-established on-line information systems, which is essential to the function of our Financial Services and Human Resources departments. This service provider has been used since 2003 and offers a significant price advantage to the suite of various products offered by Canadian vendors which would have to be purchased in order to achieve the same degree of program integration.

Universities	A (Description)	B (Conditions)	C (Reasons)
		protocols including time restrictions, audit function, and pre-approved IP addresses.	
	2. **University ID Card.** Management of access and financial processes used through the University ID Card.	2. **University ID Card.** Limited access: only where required for maintenance and troubleshooting. Contractual security measures: all personal information will be stored in Canada; restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including 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.	2. **University ID Card.** This system is proprietary in nature and is only sold and supported by this company. The University's identification card is used by all staff, faculty and students for a variety of purposes, including access to facilities, financial transactions on and off campus, and various administrative functions. Proper management of this integrated tool is necessary for the administrative functions of the University.
	3. **Employment Tool.** Comprehensive online		

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

Universities	A (Description)	B (Conditions)	C (Reasons)
		subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.	
	5. **Wireless Products.** Service provider for wireless products for employees, long distance and teleconferencing services.	5. **Wireless Products.** Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees. Internal security measures: process in place to minimize disclosure of personal information.	5. **Wireless Products.** Mobile communications solution for employees, as well as long distance calling and teleconferencing, are essential for administrative operations of the University. Significant price advantage with this service provider through the MASH sector rates negotiated by the Province.
	6. **Warranty Maintenance.** Product warranty maintenance for electronics (Storage in United States).	6. **Warranty Maintenance.** Personal information provided is limited to what is necessary for warranty coverage; where possible and applicable, personal information will be removed from products sent to service provider for maintenance or replacement. In many cases, the customer has already provided their	6. **Warranty Maintenance.** Necessary for Dalhousie's program as a supplier of the service provider's products. Since the service provider is the exclusive supplier of maintenance under warranty, there is no Canadian alternative available.

Universities	A (Description)	B (Conditions)	C (Reasons)
		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.	
	7. **Maintenance Support.** Maintenance support for product which allows University staff and faculty to schedule and manage meetings and activities in an integrated environment. (Remote access for maintenance from United States).	7. **Maintenance Support.** Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.	7. **Maintenance Support.** The ability to effectively schedule and manage meetings and activities is necessary for Dalhousie operations. This product offers superior functionality and range of service not identified in any Canadian alternatives; access rarely required.
	8. **Maintenance Support** for academic product used extensively by faculty for online teaching. (Remote access from US).	8. **Maintenance Support Measures:** restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols	8. **Maintenance Support.** The provision of online teaching opportunities is necessary to Dalhousie academic operations. This product offers a superior range of service and functionality; and has been an established service at Dalhousie for several years, therefore would require a heavy cost to convert; access rarely required.

Universities	A (Description)	B (Conditions)	C (Reasons)
		including time restrictions, audit function, and pre-approved IP addresses.	
	9. **Maintenance support** for statistical software product, used in course teaching and research (Remote access from US).	9. **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 purposes.	9. **Maintenance Support.** Necessary for Dalhousie academic and research operations in several departments. This product offers superior functionality and range of service, according to evaluations conducted by users; access rarely required.
	10. **Academic software:** supports teaching activities and allows for online collaboration, e.g.	10. **Academic Software.**	10. **Academic Software.** Necessary for Dalhousie's academic programs in a variety of disciplines; no Canadian product offers a comparable suite of products, service and functionality, combined with

Universities	A (Description)	B (Conditions)	C (Reasons)
	voice, video, application sharing, etc. (Information stored on server located in Canada, however access from the US may still be required for maintenance purposes). The product is a set of applications used for collaboration in teaching, which are fully integrated with other existing University applications. (Access from the United States). 11**. Service provider maintenance** for its hardware and software products used extensively throughout the University. Mostly done on-site, however in some cases failed equipment which may contain	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. 11. **Service provider maintenance.** Contractual measures in place to restrict access and disclosure of personal information to service provider and its employees: access to	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. 11. **Service provider maintenance.** Hardware and software from this service provider are used around the clock in University data centres and other operations, e.g. servers, switches, printers, etc. Maintenance coverage is necessary to our ability to maintain 24/7 operational requirements for these products.

Universities	A (Description)	B (Conditions)	C (Reasons)
	personal information may need to be returned to service provider in the United States. 12. **Maintenance support** for a web-based database that manages information and processes related to student work experience placements in industry. (Remote access from US). 13**. Maintenance support** for product which allows for real-time synchronization of faculty and staff calendars with wireless tools. (Remote access from US).	university systems will be subject to Dalhousie protocols including time restrictions, on-site security, and audit function. Where possible, personal information will be removed from products which require service. 12. **Maintenance support. Contractual Security Measures**: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses. 13. **Maintenance support. Contractual Security Measures:** restrictions on access to and disclosure of information by service provider and employees;	12. **Maintenance support**. Effectively managing information and processes for student work placements is necessary for the operation of Dalhousie co-operative education programs, particularly in Architecture, Commerce, Computer Science, and Engineering. Cost prohibitive for Canadian alternative; access rarely required. 13. **Maintenance support.** Making calendars available on the wireless tools used by the faculty and staff, who are required to use them is necessary for Dalhousie operations. There is no suitable Canadian alternative, given Dalhousie IT architecture and costs to convert; access rarely required.

Universities	A (Description)	B (Conditions)	C (Reasons)
	14. **Plagiarism Detection.** Academic program: online plagiarism detection service (Storage in US).	remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses. 14. **Plagiarism Detection**. Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; Storage of Dalhousie information will be segregated from other users; Internal security measures: process in place to minimize disclosure of personal information.	14. **Plagiarism Detection**. Necessary for Dalhousie's academic programs in order to maintain high standards of academic integrity. There is currently no product in Canada offering a comparable range of service and functionality. Minimal personal information disclosed.
	15. **Maintenance support** for product which supports all major University administrative computing applications.(Remote access from US or Bangalore, India).	15. **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,	15. **Maintenance support.** Necessary service for the operation of integral Dalhousie academic computing services; no Canadian alternative identified; access rarely required.
	16. **Maintenance support** for facilities		

Universities	A (Description)	B (Conditions)	C (Reasons)
	management product used for reserving rooms on campus, specifically for event and classroom scheduling. (Remote access from US). 17. **Maintenance support** for academic product which provides students with information regarding their progress towards meeting their degree requirements (Remote access from US). 18. **Maintenance support** for a scheduling and data tracking software, designed for university student	audit function, and pre-approved IP addresses. 16. **Maintenance support.** Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses. 17. **Maintenance support.** Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses.	16. **Maintenance support.** The ability to effectively manage room bookings across campus through one centralized program is necessary for Dalhousie operations. This product offers superior functionality to the identified Canadian alternative, and there would be a heavy cost to convert in terms of labor and acquisition costs. Access rarely required. 17. **Maintenance support.** Allowing students to access their information regarding progress towards degree requirements is necessary for Dalhousie operations, particularly in student advising and counseling, and for the Registrar's Office. No Canadian alternatives have been identified; access rarely required. 18. **Maintenance support**. Providing advising and counseling services to students, and effectively managing and tracking those services, is necessary for Dalhousie student services operations. This

Universities	A (Description)	B (Conditions)	C (Reasons)
	advising and counseling (Remote access from US). 19. **Maintenance support.** Maintenance support for student services product which allows faculty members to convey concerns to students about aspects of class performance and provide referral to on-campus resources. (Remote access from US). 20. **Evaluations.** Software product used to collect and maintain evaluations specifically in the medical education field (e.g. student evaluations, preceptor evaluations, etc.). This product was originally developed in Canada,	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. 19. **Maintenance support.** Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to Dalhousie protocols including time restrictions, audit function, and pre-approved IP addresses. 20. **Evaluations.** Data is stored internally. Contractual security measures: restrictions on	product offers superior functionality and range of service; access rarely required. 19. **Maintenance support.** The ability to identify and address potential student performance issues at the earliest possible stage is necessary for the Dalhousie operations in terms of enhancing the student experience. No Canadian alternatives identified; access rarely required. 20. **Evaluations.** Medical education evaluations are a necessary requirement of the operation of our Faculty of Medicine; proper management of these evaluations is critical to decision-making with respect to promotion throughout a student's medical education. This tool was 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

Universities	A (Description)	B (Conditions)	C (Reasons)
	however is now a wholly-owned subsidiary of a US company. Product is still maintained in Canada. 21. **Academic Software**. Service provider licenses to the University certain content in the form of digital books and provides software and technology services to make the content available to its students, faculty and administration in the field of dentistry (licensor located in US). 22. **Hardware/Software.** Lease and maintenance multifunction devises (copy/print/scan/fax devices) (vendor headquartered in Japan).	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, pre-approved IP addresses, and segregation of personal information where possible. Vendor agrees that any remote access will only occur from within Canada. 21. **Academic Software.** Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees. 22. **Hardware/Software.** Contractual security	tool for our purposes. 21. **Academic Software.** Product superior in terms of service and functionality including a complete digital library of dental content from all major publishers, in offline, online and mobile modalities. 22. **Hardware/Software.** No Canadian alternatives identified. Awarded through a tender process.

Universities	A (Description)	B (Conditions)	C (Reasons)
	23. **Website Feedback.** Online software enabling visitors to give feedback on the web pages. Feedback not tied to identifiable individual unless visitor opts to provide email address. Licensor located in Israel.	measures: restricted access to hard drive during maintenance; removed at end of lease; confidentiality agreement; internal technical controls to limit access to information network segregation; encrypted communication; limited outbound destinations; prohibited inbound connections; internal administrative controls to limited access to personal information. **23. Restricted access** through server authentication and data encryption, and no IP logging.	23. **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:** We did not store any information such as employee data, student records or other information outside		1. 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 of 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

Universities	A (Description)	B (Conditions)	C (Reasons)
	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.	2. There was no limit on 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).	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. 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 systems are the responsibility of the department chairpersons or department managers with consultation from Information and Technology and Services.
St. Francis Xavier	1. The University's financial software "Bi-Tech" is provided by a U. S. software vendor Sungard Bi-Tech since 1988. The software requires periodic maintenance and updates.	1. The University has taken steps to minimize our exposure by restricting access to our system to designated and prescheduled time periods and only when maintenance and update activities cannot be	1. The cost of switching our software vendors is cost prohibitive at this time.

Universities	A (Description)	B (Conditions)	C (Reasons)
	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.	accomplished by university personnel. We are working with mature software product and, historically, access has been for semi-annual updates only, therefore, we have minimal exposure points.	
	2. Kinetics software (Kx) is a comprehensive software programme that manages catering facility and residential bookings. It is comparable to large conference or hotel management systems. The Conferences and Special Events Department at the university uses the programme as our main software to support our	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.

Universities	A (Description)	B (Conditions)	C (Reasons)
	operations making use of the Events, Catering, Marketing and Extracts modules available within the software. 3. Course online management system. The systems stores names, student ID numbers and meal plan details. Storage is on server in Canada onsite. Remote access is only permitted when a technical issue arises that cannot be resolved.	3. Vendor provides technical support through remote means previously arranged with the university's technology support group for each incident.	3. The only method of receiving technical support is through remote access by the vendor.
Nova Scotia Agricultural College	The NSAC allows our Student Information System (SIS) provider, Datatel Inc., to provide Tier II application maintenance/support to our system which is housed on the NSAC campus. No data resides in a foreign country. The SIS is utilized by a wide variety of stakeholders including students, staff,	Administrative rights are controlled by the NSAC Database Systems Administrator with username/password authentication for TCP/IP connectivity being granted to Datatel as required. As noted above, this connectivity is restricted to a range of Datatel IP addresses. This access is monitored and compared to	When the NSAC purchased the Datatel Colleague/Benefactor system in 2004, there were no competitors in the Canadian marketplace. All three top SIS systems were provided by US vendors. This continues to be the case. Tier II support of this type of massive integrated system is typically provided by the vendor due to the breadth and depth of knowledge required for problem resolution. The vendor has a large staff of highly trained consultants, systems support staff and programmers who are experts on the integrated system and its many components (client software, database, programming language,

Universities	A (Description)	B (Conditions)	C (Reasons)
	faculty, senior management and various units/depts (e.g., Financial Services, Registry, Continuing Education, Alumni Development and External Relations, Graduate Studies Office, Residence Services). The system houses all academic and student financial account information as well as alumni and campaign information. The SIS is a mission critical system that supports the core business activities of the NSAC. Datatel is one of the leading North American SIS providers with their head office located in Fairfax, Virginia (http://datatel.com). Datatel accesses our system on a monthly basis to solve problems that are not resolved by our first level of support which is	monthly reports provided by the vendor of the work that they have performed for the NSAC. As well, Datatel's login information is periodically changed for security reasons and login information is only provided via direct communication via telephone to Datatel's head office.	systems tools, etc.). The product is also always evolving and the university needs to maintain the ongoing relationship with the vendor to take advantage of enhancements as they develop. To properly complete our daily business, the NSAC must continue to have Tier II support provided by this vendor.

Universities	A (Description)	B (Conditions)	C (Reasons)
	provided by our in-house Database Systems Administrators. All access is via TCT/IP protocol. NSAC stakeholder access is restricted to internal NSAC network connectivity, while Datatel access is provided through firewall security to a restricted range of Datatel IP addresses. All TCP/IP and firewall/security management is provided by the NS Provincial Resources Corporate Services Unit – IT Division.		

Universities	A (Description)	B (Conditions)	C (Reasons)
Nova Scotia College of Arts and Design (NSCAD)	Moved from various systems including to a single unified Enterprise Resource Planning (ERP) system provided by Datatel Inc. of Fairfax, VA.	Access to personal information is to be limited to Datatel personnel providing support for the ERP system using remote access technology in case of issues with the system. All data will remain resident on NSCAD University servers located in Nova Scotia.	All major academic ERP vendors (Datatel, Sungard and PeopleSoft) are based in the United States. To design and implement a home-grown ERP system would be cost-prohibitive for an institution NSCAD University's size.
Nova Scotia Community College	1. **Storage:** The Nova Scotia Community College has allowed for the storage of personal information under its control to be held by Hobsons EMT (formerly Apply Yourself, Inc.). This company is located in Fairfax, Virginia (USA). Hobsons EMT is an application service provider offering web-based data management storage for the College's on-line application	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. 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. Since our last submission, we investigated service providers within Canada, however, there were no emerging or known Canadian companies identified by us through the usual channels – conferences, trade shows or vendor contacts. The College continues to seek on-line application solutions through products and functionality available with our current database service provider (Oracle/PeopleSoft) and products. Currently, a solution is in the early adopter stage (Oracle/PeopleSoft) and may be ready to investigate fully towards possible purchase in 2011.

Universities	A (Description)	B (Conditions)	C (Reasons)
	process. 2. **Travel:** The College will allow our employees to transport personal information temporarily outside Canada. Transport is only to the extent that it is strictly necessary for their assigned duties or as a necessary part of a research project. 3. **Accessing personal information in College data repositories from outside Canada**.	2. **Travel:** This information will be transported using cellular telephones, wireless handhelds, laptops and storage devices. 3. The College will permit its employees to use web-based or other internet access tools if it is a necessary part of performing his or her assigned duties or as a necessary part of a research project.	2. **Travel:** Employees will be required to take all reasonable precautions (e.g., encryption) to protect personal information.

Table 4[4]: January 1 - December 31, 2010 Foreign Access and Storage by School Boards

School Boards	A (Decision)	B (Conditions)	C (Reasons)
Annapolis Valley Regional School Board	One individual residing in the U.S. has access to a server owned by the AVRSB. The server is housed in Canada. The server stores Educator's Handbook/Student Discipline Referral software and related student data. The individual with access to this server/software is the author of this software. This software is in use by one school but will be discontinued in the 2011-2012 school year.	Access is permitted only when necessary for maintenance or upgrading of software.	This software is necessary for day-to-day work of teachers in schools and for AVRSB monitoring purposes, in order to track and report student discipline issues. This software was determined to be the best option at reasonable cost to perform these functions. This software will be discontinued in the 2011-2012 school year.
Cape Breton-Victoria Regional School Board	Approximately eight staff members travelled outside Canada and may have, or had the ability to, access personnel information via remote email, blackberry and/or personal computer.	All personnel information is housed on-site with existing infrastructure. All blackberries and personal computers are password protected.	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 e-mail

[4] Chignecto-Central Regional School Board and Conseil scolaire acadien provincial did not store or have access to personal information outside of Canada.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
			for decision-making and information purposes.
Halifax Regional School Board	Twenty-five (25) staff members travelled outside of Canada, which would have had access to person information via their Blackberries or laptop computers.	Relevant HRSB policies would apply to Blackberry and computer usage outside of Canada. Each Blackberry and computer is password protected. The HRSB will incorporate into its policy direction on access and storage of personal information outside to Canada.	Staff members, at issue, occupy management positions and must be available by e-mail for decision-making and information purposes.
Strait Regional School Board	The Strait Regional School Board currently hold on-line subscriptions for United Streaming and Reading A to Z. These are on line subscriptions to education media. The teacher's name and school are provided to both on line education media providers. This contract has been in existence prior to December 15, 2006. To our knowledge, twenty seven (27) employees travelled outside of Canada and may have (or had the ability to) accessed personal information via remote email, BlackBerry,	The Strait Regional School Board has restricted employees to travel outside of Canada with board owned equipment. Employees are required to obtain prior written consent of the head of the Public Body to transport Board owned equipment outside of Canada. The SRSB network allows secure VPN access only.	Consent to transport Board owned equipment outside of Canada is provided only in instances when it is deemed necessary for management and operations.

School Boards	A (Decision)	B (Conditions)	C (Reasons)
	personal computer or by any other means.		
Tri-County Regional School Board	Tri-County Regional School Board reported that no personal information was accessed or retained outside of Canada.		

Table 5 January 1 – December 31, 2010 Foreign Access and Storage by Municipalities[5]

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
Municipality of the County of Colchester	Seven staff members travelled outside Canada during calendar 2010. It is known that two staff could have accessed personal email or stored information and email through GroupWise, via a laptop or Blackberry. Both employees indicated that they didn't.	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 travel for business or personal reasons, they may be expected to monitor their business email in order to fulfill their job responsibilities.
Municipality of the County of Kings	The Manager of Engineering & Public Works travelled to Texas between March 27, 2010 and April 5, 2010.	Email access requires authentication through secure login/password.	The Management Team determined that access to email was necessary for the Manager of Engineering to make informed decisions on key operational issues while out of the country.

[5] Guysborough County Regional Development Authority, NS Association of Regional Development Authorities and Strait-Highlands Regional Development Agency, Municipalities of the Districts of Argyle, Yarmouth, Lunenburg, Chester, Guysborough, Barrington, St. Mary's, Municipalities of the Counties of Inverness, Annapolis, West Hants, East Hants, Cumberland, Pictou, Victoria, Towns of Parrsboro, Wolfville, Springhill, Westville, Pictou, Oxford, Middleton, Mahone Bay, Bridgewater, Windsor, Stellarton, Kentville, Truro, Antigonish, Bridgetown, Annapolis Royal, Stewiacke, Lockeport, Trenton, Shelburne, New Glasgow, Port Hawkesbury, Lunenburg, Amherst, Hantsport, Digby, Berwick, Clark's Harbour, Mulgrave, Cape Breton Regional Municipality, Municipality of Antigonish, Clare; Lunenburg Queens Regional Development Agency, Region of Queens Municipality and Cape Breton County Economic Development Authority had no access or storage outside of Canada to report.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
Municipality of the County of Richmond	Municipal property owners living outside Canada are sent property tax invoices twice per year (issued April 1 and September 1 of each year) by the Municipality. Information related to these invoices and related properties are regularly exchanged with property owners via mail.	Municipal property owners living outside Canada are sent property tax invoices twice per year (issued April 1 and September 1 of each year) by the Municipality. Information related to these invoices and related properties are regularly exchanged with property owners via mail.	This is required for the timely operations of the Municipality and occurs on an ongoing basis.
Halifax Regional Municipality	1. Between January 1st and December 31st, 2010, one hundred and one (101) 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). 2. The following vendors - Versaterm (Police RMS, CAD 911), Hansen (Tax Bill, Customer Service, Permit/License),	1. Prior to travelling, staff were advised that HRM communication tools (Cell Phones, Blackberries, Laptops, Memory Sticks, VPN) were to be password protected. 2. Vendor access is controlled and monitored by IT Support staff.	1. The HRM staff, who were approved for travelling 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 fulfill operational responsibilities/requirements. 2. Vendor access is necessary for the systems to continue to function properly.

Municipalities	A (Decision)	B (Conditions)	C (Reasons)
	Open Text (Document Management), Hastus ERP (Metro Transit) and RIVA (PSAB Compliance -Financial) - were provided access on an approved, need basis to the applicable production systems for support and maintenance		