Personal Information International Disclosure Protection Act

2013 Annual Report

NS Information Access and Privacy Office
June 30, 2014

Message from the Minister of Justice

I am pleased to provide the eighth Annual Report regarding public body decisions to permit foreign access and storage of personal information, as authorized under the *Personal Information International Disclosure Protection Act (PIIDPA)*. *PIIDPA* was created to enhance provincial privacy protection activities and respond to Nova Scotian concerns about the vulnerability of public sector and municipal personal information holdings to foreign access, storage and disclosure. The Act prohibits public sector entities, municipalities and their service providers from allowing foreign storage, disclosure or access to personal information, except to meet the approved "necessary requirements" of public sector or municipal operations.

Under *PIIDPA* subsection 5(3), Nova Scotia public sector and municipal entities are required to report the decision and description of any foreign access and storage of personal information occurring from January 1, 2013, to December 31, 2013, to the Minister of Justice. This report is based on the *PIIDPA* reports received by the Nova Scotia Information Access and Privacy Office.

This report contains a summary of the 69 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: 59 entities reported that there was no access or storage outside of Canada for the 2013 calendar year.

Original signed by

The Honourable Lena Metlege Diab, ECNS
Minister of Justice and Attorney General

Table of Contents

Key to 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.

Link to previous Annual PIIDPA Reports http://novascotia.ca/just/IAP/resources.asp

Government Departments[1]

Department of Agriculture

Description

1. Remote Access via Blackberry. There were six (6) instances in which staff members were approved to take blackberries while travelling outside Canada and may have accessed personal information contained in e-mail via Blackberry.

2. In the fall of 2010, Laboratory Services launched a new Veterinary Laboratory I formation System (V-LIMS) called VADDS to replace an antiquated system. While the OCIO recognized the limited options available for a new V-LIMS system, they were cautious about the security of the system on their server. CIO's security coordinator agreed to allow the vendor to host our data on their secure data server as there were no resources available to maintain it internally. To date, there have been no known breaches of the system; it functions flawlessly; and we hope to maintain this relationship.

Conditions

1. Permission must be granted in order to take a blackberry out of the Country. Remote access to e-mail is protected by username/password authentication and is delivered over a secure server link (SSL) encrypted link. All blackberries must be password protected.

2. The vendor, VetStar, has a secure server environment and the application can only be accessed by staff having an active account and password. In terms of data, there is personal data, including client names and addresses, as well as the results of any tests conducted by the lab. These results are from tests on food samples for food safety or from veterinary pathology reports. Aside from contact data, there is no human or personal health data and no financial data.

[1] Aboriginal Affairs, Acadian Affairs, African Nova Scotian Affairs, Elections Nova Scotia, Gaelic Affairs, Nova Scotia Health Research Foundation, Nova Scotia Human Rights Commission, Nova Scotia Legal Aid Commission, Nova Scotia Provincial Lotteries and Casino Corporation, Nova Scotia Public Service Long Term Disability Plan Trust Fund, Office of the Police Complaints Commissioner, Department of Seniors, Planning and Priorities, Waterfront Development Corporation had no access or storage outside of Canada to report.

Reasons

1. When staff travel, they may be required to conduct business or maintain contact with operations.

2. OCIO's security officer allowed the Department of Agriculture to establish this relationship. The assumption is they are aware of requirements pertaining to the type of data collected.

Bridge Commission

Description

See 2012 Annual PIIDPA Report.

Conditions

See 2012 Annual PIIDPA Report.

Reasons

See 2012 Annual PIIDPA Report.

Chief Information Office

Description

1. CIO staff carried assigned end-user devices outside the country on government business, with pre-approval of the Associate Deputy Minister.

2. Tangoe Inc. is under contract by NS to supply / support the Expense Management System (EMS) that the Province uses to track / manage telecommunication re-billing costs on a monthly basis. Tangoe occasionally requires remote access to the EMS application and database at PNS Datacentre to perform scheduled support or troubleshooting. Access takes place from Tangoe's Dallas, Texas offices using secure virtual private network software that also runs on a server at the PNS Datacentre. Remote access is always controlled and monitored by CIO staff.

Conditions

1. End-user devices utilized by CIO staff outside the country were protected by passwords, encryption (in some cases) and by all the security means established by the Province. CIO staff, who travel for personal reasons outside of Canada, are not approved to take government end-user devices with them unless there are no other staff with equivalent skills to sustain service delivery in his/her area. When this situation occurs, both Associate Deputy Minister and Deputy Minister approval is given.

2. The controlled remote access gateway that allows Tangoe Inc. to view the EMS database does not give the company the ability to remove or copy any files. CIO staff disable access to the database once each occurrence of remote access by Tangoe is completed. Tangoe covenants by agreement that it will comply with service-provider obligations under PIIDPA and will strictly enforce the security arrangements required to protect personal information to which it has access. Tangoe must also confirm details of those security arrangements when requested to do so by PNS. PNS staff may at any time travel to Tangoe's offices to inspect the security measures Tangoe has in place.

Reasons

1. CIO staff attending business events outside Canada may be approved to take assigned end-user devices with them to ensure seamless workflow and service continuity. Staff, approved to take devices on non-government related travel outside Canada, are only contemplated when there is a staff related single point of failure for a particular operational service and a risk of significant service disruption exists.

2. Tangoe was the best option to ensure PNS telephone billing requirements could be met. Tangoe's prior experience with other PNS telephone billing systems lowered the risk associated with support of the EMS system. There is currently no alternative method of receiving technical support access for EMS within Canada.

Communications Nova Scotia

Description

1. Google Analytics (GA) is the corporate standard for web analytics. Conditions or restrictions that have been placed on storage or access of personal information outside of Canada include: Internet Protocol (IP) addresses will be 'masked', the last series of numbers in the IP address will be removed before being stored by GA, which reduces the ability to identify specific users' behavior on our websites. The GA software does not allow government staff access to individual IP addresses. Access to the analytics information will be controlled by password, and the information will only be presented in an aggregated form. Under the Province of Nova Scotia privacy policy, IP addresses are considered personal information. The CNS Marketing Division used Google Analytics prior to the implementation of IP masking. Since fall 2012, all government websites including three Internet-related initiatives: Nova Scotia Life, Pomegranate, and Canada's University Capital, have used Google Analytics using the IP masking protocol. In the case of Google Analytics, Google collects the IP address from the visiting computer, without CNS acting in the middle, then stores a partially obfuscated (partially redacted) or masked IP outside of Canada, and uses this for analysis. Individual IP addresses are not kept or disclosed. CNS and other government departments do not even see these partial IPs, only receiving analyzed, aggregate information. The departmental privacy statements located on each website are updated to reflect CNS use of Google Analytics and will include an opt out feature for users. To summarize, CNS never collects or see IPs or partial IPs. CNS is responsible for the government Twitter, Facebook, YouTube and Flickr accounts, which are based in the U.S. These accounts are used for sharing government news releases, videos, photos and other information to a broader audience. Four employees travelled in the United States with BlackBerrys and two iPads for business. The equipment was used by only them and password protected.

Conditions

1. This information is subject to the Google Privacy Policy. (The Google Privacy Policy outlines its responsibility to protect any personal information it collects against any unauthorized access, disclosure, or destruction. It further details that they will not share any personal information without prior consent unless it is to comply with applicable laws.) CNS uses social media platforms to share information and public engagement. No IP addresses are provided or collected. CNS retweets other government accounts and public safety information from partners (RCMP, Halifax Regional Municipality, etc.) CNS does not retweet personal accounts. Facebook shares are treated in the same manner. The equipment was accessed by Communications Nova Scotia employees.

Reasons

1. Communications Nova Scotia is accountable in the 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. Social media platforms are used to increase public awareness and engagement and to correct erroneous information. It is also used to monitor public opinion which helps government to make better informed decisions regarding policy, program and service delivery. BlackBerrys were necessary to make calls and use e-mail, iPads were used to e-mail, post messages on Facebook and access Twitter.

Communities, Culture and Heritage

Description

1. Decision to allow primary service provider (Unisys Canada Inc.) for Internet resource NOVA SCOTIA HISTORICAL VITAL STATISTICS ONLINE (NSHVSO) operated by NS Communities, Culture and Heritage (Archives Division), to outsource to service sub-provider (Skipjack, Cincinnati, Ohio, USA), part of the transaction processing, and storage during processing, of credit card information collected from service clients during online interactive commercial activity.

2. Decision to launch and maintain a Flickr site, titled 'Nova Scotia Archives Photostream' and registered as http://www.flickr.com/people/nsarchives. Contents on site feature public-domain content uploaded to the site. Link on NSARM Website enables Internet visitors to access the photostream without a Flickr account. Visitors are also able to comment on content via phone or e-mail to NS Archives, rather than on Flickr site.

3. Nova Scotia Provincial Library (NSPL) maintains an integrated library system (ILS) on a cost-recovery basis for a consortium consisting of 66 branch libraries in eight regional library systems, and four government department libraries. The ILS provides a library catalogue, a purchasing module, and a circulation module (check-in/check-out, and client information). The ILS is mission critical for day to day operations of libraries. Without the ILS, libraries could not function.

The ILS contains personal information about identifiable individuals (library clients in Nova Scotia), including name, address, telephone number and email address. This personal information is voluntarily obtained when a client registers for a library card. Attached to the client's account number are titles currently on loan to the individual, those for which the individual has been billed and/or has paid and those which the user has requested. Transaction logs, maintained by NSPL, CCH, 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.

4. Nova Scotia government websites were cleared to use Google Analytics as long as it is in a manner that abides by the methodology outlined in the Privacy Impact Assessment signed by all Deputy Heads.

5. Continued use of Twitter and Facebook accounts (see 2012 PIIDPA Report)

6. Decision to allow 23 employees to travel outside Canada with Blackberry devices.

Conditions

1. No disclosure to, or retention of credit card personal information by service sub-provider outside Canada except as required to carry out and verify online commercial transactions with NSHVSO service clients.

2. N/A

3. NSPL has implemented reasonable security measures to protect personal and other information in the ILS. The ILS software is maintained on a secure server in Brunswick Place. The contract with the company stipulates that NSPL staff must be contacted when the company requires access to the ILS server. The contract with SirsiDynix was updated recently to strengthen privacy protection and to codify data access permissions. NSPL enable 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. Due to these precautions, the risk of access to personal information about Nova Scotians by SirsiDynix is low, but it is technologically feasible.

This fiscal year, NSPL conducted a retroactive Privacy Impact Assessment to thoroughly understand exactly what information is collected by each regional library system, how it is used, as well as the different interactions that occur when multiple users access the system. A PIA had not been done before as the system was in place prior to legislation requiring one be completed. Any issues that were discovered were quickly addressed by NSPL and the appropriate regional library board.

4. N/A

5. N/A

6. Blackberry devices are password protection following guidelines by CIO.

Reasons

1. Commercial component of NSHVSO online service depends on client's ability to prepay for copies online via credit card transaction conducted in real time. Due to the global character of today's financial services industry, it is extremely unlikely that online credit-card transactions can be completed and verified without the personal information collected during transaction processing being stored, accessed from or disclosed outside of Canada.

2. N/A

3. The decision was made to continue with SirsiDynix because there is no Canadian alternative. There are four major ILS vendors in the world that offer systems with the functionality required by libraries in the NSPL consortium, none of which are Canadian companies. When NSPL chose Sirsi in 2003, the company was a Canadian corporation. In 2005, Sirsi was purchased by Dynix, an American company, and became SirsiDynix. The company serves customers worldwide from its base in the United States.

4. In keeping with Strategic Goal 3 of the Departmental Web Strategy: Provide timely and reliable intelligence that includes regular statistical monitoring and reporting (web analytics).

5. In keeping with Strategic Goal 2 of the Departmental Web Strategy: Created a content rich, well-designed, easy to navigate, relevant and accessible online presence across the department that is user-centered. Social media initiatives will be attached to a clear business driver (communications, outreach, recruitment, program delivery, consultation, employee engagement, workplace collaboration). For the most part, social media initiatives (Web 2.0) will be launched to drive visitors to Web 1.0 sites.

6. Blackberry devices were necessary to make calls and use e-mail.

Community Services

Description

1. Since 2000, Community Services has stored approximately 8000 boxes of records with Iron Mountain (an archival services and storage centre). The type of records stored at Iron Mountain covers a wide variety of records and some of these records contain personal information of Nova Scotians. While the records are stored at a facility in Nova Scotia, the database maintained by Iron Mountain is accessible in the U.S.

2. Since 2002, Housing Nova Scotia (formerly the Nova Scotia Housing Development Corporation) has contracted Yardi Systems, Inc. under an alternate services provider (ASP) agreement to provide Tier II application support and maintenance as well as to manage the application hardware configuration necessary to operate the application. Tier II application support is provided by the Yardi Canadian offices operated in Mississauga, Ontario once issues reported are vetted by NS Department of Community Services IT Services 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. See description of access or storage provided in the 2012 annual PIIDPA report.

3. During the 2013 calendar year, there were six children in care placed in residential treatment facilities in the U.S. to receive residential treatment services. (See the 2012 Annual PIIDPA Report for more details).

Conditions

1. The data contained in the Iron Mountain database does not contain any personal information. The database is set up with box number information of Community Services. All searches using personal information is done at Community Services. This search would result in a box number matching the personal information. Then, it is only the box number information that is provided to Iron Mountain to identify the Community Services box. Community Services never requests the individual file to be pulled from the box, but rather requests the entire box be sent to us when needed.

2. Under the terms of the contract, Yardi agrees that it will not 'use, disseminate or in any way disclose any of the confidential information' of the Nova Scotia Housing Development

Corporation [Housing Nova Scotia] to 'any person, firm or business, except to the extent it is necessary' to perform its obligations or exercise its rights. See description of access or storage provided in the 2012 annual PIIDPA report.

3. See the 2012 Annual PIIDPA Report for more details.

Reasons

1. The decision dates back to August 2000, pre-dating PIIDPA requirements and was necessary at that time to meet the Departments storage requirements. Community Services is taking steps to address the volume of boxes/records at Iron Mountain with the hopes of significantly reducing the number of boxes being stored at their facility.

2. Before entering into this arrangement, staff from the Housing Authorities (an agent of the Nova Scotia Housing Development Corporation) and the Department of Community Services underwent an RFP process and, through a structured evaluation process of the proposals received, determined that the Yardi Systems software operated under an ASP agreement was the best solution. The software provided the best business functionality based on criteria defined at the time of the RFP process for the costs proposed. The technical framework proposed to operate this software was deemed acceptable based on criteria defined at the time of the RFP process for the costs proposed.

3. See the 2012 Annual PIIDPA Report for more details.

Economic and Rural Development and Tourism

Description

The Nova Scotian Tourism Agency requires an easy-to-use, password protected system that can be accessed by its external partners in marketing. MailChimp is an e-mail marketing device which allows users to sign up to receive Nova Scotia tourism marketing information via e-mail. All information is stored on the MailChimp server located in the U.S. There are currently no Canadian providers of this service, which meet NSTA's usage requirements.

Conditions

The e-mail address is provided voluntarily for this purpose. A confirmation e-mail is sent from NSTA and must be replied to before the name can be added to the database. Information can be used only for its specified purpose. NSTA has the capacity to download the information and delete the MailChimp account if necessary. If site is abandoned, MailChimp may delete the information after one year. If information in a MailChimp account appears to have been used without appropriate confirmations and consent, the account will be frozen.

The information is password protected. MailChimp has policies in place to prevent spammers from using their site and to identify and delete abandoned or terminated accounts.

Reasons

This service is an essential component of NSTA's internet marketing strategy. Individuals will be informed that their information is stored outside Canada pursuant to Section 5(1)(a).

Education and Early Childhood Development

Description

1. Provincial Student Information System: The Provincial Student Information System (SIS) is used by the Nova Scotia education system (schools, school boards, Department of Education and Early Childhood Development) to manage school operations, including processes such as student registration and enrolment, attendance, student scheduling, behaviour, student progress, individual program plans, and school accreditation. In addition, the system is used to analyze and report on student achievement and other vital student, school, and program data for policy and program decisions. The SIS contains personal information regarding students and parents, including names, addresses, phone numbers, email addresses, medical, behavioural incidents, and academic records. This information about students and parents is necessary for the Nova Scotia education system to manage student enrollment and education from grade primary through high school.

2. TIENET: The Extended Services and Programming system is a component of the provincial Student Information System and is used by the Nova Scotia education system (schools, school boards, Department of Education and Early Childhood Development) to manage the student documentation associated with the Program Planning Process such as Individual Program Plans, Documented Adaptations, Health/Emergency Care Plans, Special Transportation Needs and SchoolsPlus information. The system contains personal information regarding students and parents, including names, addresses, phone numbers, email addresses, medical, program planning and academic records. This information about students and parents is necessary for the Nova Scotia education system to manage student program delivery in the areas noted above for students in Grade Primary to 12.

3. Teacher Certification Fee Processing: The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the U.S. for payment authorization and reconciliation. Personal information that is transmitted through or stored outside Canada is at risk of a foreign demand for disclosure.

4. Teacher Summer Professional Development Registration System: The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the U.S. for payment authorization and reconciliation. Personal information that is transmitted through or stored outside Canada is at risk of a foreign demand for disclosure.

5. Travel with electronic devices: A number of staff traveled outside Canada for business and/or pleasure and had the ability to access personal information contained in email or stored in the Microsoft Outlook email system using devices including cell phones, iPads, BlackBerrys and laptops. Staff seek permission from the head of the public body before taking devices across the Canadian border.

6. Use of Social Media: The Department operates a Twitter account. Twitter is based in the U.S. This account is used for sharing government news releases, videos, photos and other information to a broader audience.

7. International Programs - Transcript Payment Service: The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the U.S. for payment authorization and reconciliation. Personal information that is transmitted through or stored outside Canada is at risk of a foreign demand for disclosure.

8. Fleet Focus (Fleet Management, TPW) with headquarters in Calgary, AB were provided access on an approved need basis to the applicable production systems for support and maintenance purposes.

9. EMC (Storage Area Network, VMWare) with headquarters in Toronto, ON were provided access on an approved need basis to the applicable production systems for support and maintenance purposes.

10. City Watch (Public Safety Notification) with a headquarters in Bloomington, MN were provided access on an approved need basis to the applicable production systems for support and maintenance purposes.

11. Safran Morpho (Digital Mug System) with headquarters in Montreal, QC was provided access on an approved need basis to the applicable production systems for support and maintenance purposes.

12. Microsoft (Email, Office, Sharepoint, File Shares) with a headquarters in Mississauga, ON were provided access on an approved need basis to the applicable production systems for support and maintenance purposes.

13. Research in Motion (Blackberry) with headquarters in Waterloo, ON were provided access on an approved need basis to the applicable production systems for support and maintenance purposes.

14. Service Providers - Service Now, IT Service Relationship Management with headquarters in Santa Clara, CA. HRM's data is hosted in Canada.

Conditions

1. The Department of Education and Early Childhood Development 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 and Early Childhood Development, Brunswick Place, Halifax, NS. The contract with the service provider (Pearson School Systems) stipulates that Department of Education and Early

Childhood Development staff will authorize access to the environment by Pearson technical staff located in Rancho Cordova, California, USA, for the purpose of providing periodic technical support. Such access will be limited to predetermined time periods, at the end of which access is terminated by Department staff. Department staff monitor and audit to ensure the access is reasonable and appropriate. Pearson has no operational requirements to access personal information about clients. Therefore, the risk of access to student and parent's personal information by Pearson is low, but it is technologically possible.

2. The Department of Education and Early Childhood Development has implemented reasonable security measures to protect electronic storage of personal and other information in the Extended Services and Programming system. The information and software are maintained in a secure environment housed at the Department of Education and Early Childhood Development, Brunswick Place, Halifax, NS. The contract with the service provider (MAXIMUS) stipulates that Department of Education and Early Childhood Development staff will authorize access to the environment by MAXIMUS technical staff located in Eatontown, New Jersey, USA, for the purpose of providing periodic technical support. Staff monitor and audit to ensure the access is reasonable and appropriate. MAXIMUS has no operational requirements to access personal information about clients. Therefore, the risk of access to student and parents' personal information by MAXIMUS is low, but it is technologically possible.

3. The Online Payment System has been developed in adherence with government and departmental security standards to ensure system access is restricted to authorized individuals and information is protected against unauthorized disclosure. Cardholders have agreed to the card issuing institutions' privacy statements that include a notice that third party service providers may be used to process credit card transactions.

4. The Online Payment System has been developed in adherence with government and departmental security standards to ensure system access is restricted to authorized individuals and information is protected against unauthorized disclosure. Cardholders have agreed to the card issuing institutions' privacy statements that include a notice that third party service providers may be used to process credit card transactions.

5. Remote access to staff email accounts through GroupWise and Microsoft Outlook is protected by username/password authentication and is delivered through a combination of VPN and encryption.

6. The Department uses Twitter to share information and interact online with the public and organizations in social spaces. The Department collects no IP addresses or personal information through these services. The Department retweets other government accounts and public safety information from partners (RCMP, Halifax Regional Municipality, school boards, etc.) Photos and videos that are posted to all social media platforms have written consent from the people in them where required.

7. The Online Payment System has been developed in adherence with government and departmental security standards to ensure system access is restricted to authorized individuals and information is protected against unauthorized disclosure. Cardholders have agreed to the card issuing institutions' privacy statements that include a notice that third party service providers may be used to process credit card transactions.

8. Vendor access is controlled and monitored by IT Support staff.

9. Service providers are bound by duly executed agreements that detail their obligations for the protection, use and disclosure of personal information.

Reasons

1. The decision to contract with Pearson for provision of the Student Information System was reached after an extensive evaluation of vendor products through a tendering process. Pearson was chosen due to its superior functional capability in meeting the requirements of the Nova Scotia education system, as well as its standing as a leading distributor of Student Information System software worldwide.

2. The decision to contract with MAXIMUS for provision of the Extended Services and Programming system was reached after an extensive evaluation of vendor products through a public tendering process. MAXIMUS was chosen due to its superior functional capability in meeting the requirements of the Nova Scotia education system as well as its standing as a leading distributor of Special Education Case Management software worldwide.

3. Teacher Certification offers the option of payment by credit card payments as a convenience for teachers and to provide efficient and effective online services.

4. The option of payment by credit card payments is a convenience for teachers and provides efficient and effective online services.

5. Staff are expected to monitor their email and voicemail for business continuity purposes and maintain contact with operations. BlackBerrys were necessary to make calls, access email and Internet sites and make telephone calls. Laptops and iPads are needed for preparing documents and accessing email and Internet sites.

6. Social media platforms are used to engage the community, increase public awareness and to promote the dissemination of accurate, timely information.

7. The option of payment by credit card is a convenience for students and provides efficient and effective online services especially where the students are located around the world.

8. Vendor access is necessary for the system to continue to function properly.

9. Service providers were secured through the RFP process and achieved the highest overall proposal evaluation scoring and provided the best financial value for the municipality.

Energy

Description

1. Twenty-three employees were authorized to access their email or bring a device while travelling outside of Canada on business or personal travel. Individuals used their government issued cellular phone or remote Outlook to access their Government email account from a computer. Individuals may also travel with a government laptop computer.

Conditions

1. Staff use of Blackberry devices provides email delivered over an SSL-encrypted link via the secure BlackBerry server. Blackberry devices and laptops are password protected. Remote access to staff email accounts through remote Outlook is protected by username/password authentication over an HTTPS secured connection. All laptops are protected with a username and password authentication process.

Reasons

1. Staff may be required to monitor their email and voicemail for business continuity purposes. BlackBerry devices were necessary to make calls and access email while travelling. Laptops are required for preparing documents, accessing email and Internet sites. Staff use of remote web access to government email provides business continuity for certain roles.

Environment

Description

1. Two employees travelled outside of Canada with a Blackberry.

Conditions

1. Permission was granted in order to take a Blackberry out of the Country. All devices used during travel outside of Canada were password protected.

Reasons

1. Blackberries were necessary to make calls and access email for business continuity purposes.

Executive Council

Description

1. Three employees took their electronic devices outside the country with the permission of their Deputy Head.

Conditions

1. N/A

Reasons

1. In accordance with PIIDPA, employees were permitted to take electronic devices out of the country to meet the requirements of the department's operation and / or the performance of their duties.

Film and Creative Industries Nova Scotia

Description

1. Approximately two representatives traveled outside Canada on business. These representatives had the ability to access personal information carried on email or stored in Outlook via remote access (Blackberry and laptop) to the Outlook email system.

Conditions

1. N/A

Reasons

1. When staff travel outside Canada for business reasons, they are expected to monitor their email in order to fulfill their job responsibilities.

Finance and Treasury Board

Description

1. The Department operates SAP systems for the public sector including provincial departments, school boards, regional housing authorities, district health authorities and IWK Health Centre, NSLC and several municipal organizations. It is necessary that remote access to public sector SAP systems be performed by SAP support staff via secure network connections to provide routine and emergency support maintenance. Following a highly audited and controlled management approval process, access to SAP systems occurred several times throughout the reporting period as required to correct or troubleshoot various problems within the SAP systems. Access was only from SAP's own secure internal support network and carried out by SAP staff resident in SAP service locations such as the U.S., Ireland, Brazil, Germany and India.

2. Remote Access via Blackberry or other electronic devices. There were nine instances where staff were approved to take their Blackberry or other electronic device while travelling outside Canada and may have accessed personal information.

3. Royal Bank of Canada (RBC) was awarded a contract in 2010 by the Province to provide electronic vendor payments to U.S. vendors/individuals for the period Feb 2013 to Jan 2016.

Conditions

1. 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 SAP Service Management and all access activity is recorded in an audit log so that verification can be done of whether personal information has been accessed. In addition, this access occurs over secure network connections that must be opened to allow SAP to enter a specific system. This secure network connection also prevents other parties from gaining unauthorized access to the SAP systems. This type of remote access very rarely involves actual access to personal information and is typically limited to system operations information. In cases where approved access does involve potential access to personal information for the purposes of resolving a specific support problem, records and audit logs of that access are maintained. In all cases where access was granted to SAP support staff, specific controls on the time and duration of that access are maintained. There is no storage of data from SAP systems outside Canada.

2. Permission must be granted in order to take a Blackberry or Laptop out of the Country. Remote access to e-mail is protected by username/password authentication and is delivered over a secure server link (SSL) encrypted link. All devices must be password protected.

3. RBC has entered into a service agreement with the Province. The terms set out consider the automated clearing houses (ACHs) required to process electronic vendor payments outside Canada. RBC is required to report to the Minister all unauthorized access or foreign disclosure of personal information. All Automated Clearing House (ACH) Payments are governed by the National Automated Clearinghouse Association (NACHA) because of the sensitivity of the data in the files. Use of ACH data for purposes other than to complete the transfer of the funds is not endorsed by NACHA and in some cases may be illegal. Each bank in the U.S. must comply to the rules of NACHA Vendors opt into receiving electronic payments. They are required to complete an application form consenting to have payments forwarded to them via our electronic vendor payment (EVP) system.

Reasons

1. Access by SAP support staff is required from time to time in order to assist the SAP Service Management 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 SAP Service Management 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 SAP Service Management Division in the performance of services to various public sector organizations who use SAP.

2. When staff travel, they may be required to conduct business or maintain contact with operations.

3. Electronic vendor payments provides a low cost, flexible and highly reliable payment system to vendors. The requirement to electronically forward funds to vendors located in the U.S. requires that information flows through an Automated Clearing House. There is no ACH that stores information in Canada.

Fisheries and Aquaculture

Description

1. There were five instances in which staff members were approved to take Blackberries while travelling outside Canada and may have accessed personal information contained in e-mail via Blackberry.

Conditions

1. Permission must be granted in order to take a Blackberry out of the Country. Remote access to e-mail is protected by username/password authentication and is delivered over a secure server link (SSL) encrypted link. All Blackberries must be password protected.

Reasons

1. When staff travel, they may be required to conduct business or maintain contact with operations.

Health and Wellness

Description

There were no approvals granted for the storage of personal information in the custody or control of the department outside of Canada.

The department granted the following approvals for access to personal information in the custody or control of department:

1. Language Line Services – HealthLink 811
Language Line Services was sub-contracted by McKesson Canada (HealthLink 811 Operator) to provide telephone based language interpreter services for callers whose first language is not English. Language interpreters may be located in any one of a number of countries in or outside North America. The key piece for clarification is that calls involving interpreters are not audio recorded outside of Canada nor do the interpreters document any details of the call, therefore, no recorded information is collected or stored outside of Canada.

2. Relay Health
In rare circumstances, Relay Health will require remote access to the information system for tier three level technical support to 811 applications. When Relay Health in the U.S. is required for this level of support, they are consulted by local 811 technical support to address related requirements and gain access to the system and associated information.

3. McKesson Corporation, Secure Health Record (SHARE)
McKesson developers need to access the provincial Electronic Health Record (SHARE) system from their offices, outside of Canada to deploy the software changes and test the upgrade software.

4. McKesson Corporation, Relay Health solution:
Personal Health Record (PHR) Pilot Project
In rare circumstances, Relay Health will require remote access to the information system for tier three level technical support to the PHR application. When Relay Health in the U.S. is required for this level of support, they are consulted by local Relay Health technical support to address related requirements and gain access to the system and associated information.

5. 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 on-going maintenance of the FairWarning application; this includes having access to the application audit log database that contains limited personal information. FairWarning may also assist in providing FairWarning application training to District Health Authority Privacy Leads and other appropriate DHA / Department of Health and Wellness / HITS-NS staff using the application and audit log data.

6. DHW Employee Access:
Between January 1, 2013 to December 31, 2013 twenty-one (21) staff of the Department Health and

Wellness traveled outside Canada on business and had the ability to access personal information carried on e-mail or stored in GroupWise via remote access to the GroupWise system.

Conditions

1. Language Line Services – HealthLink 811
Language Line obtains a signed confidentiality agreement from each respective interpreter and reviews these agreements once annually. The interpreter service is provided over the phone. Language Line Services, as per McKesson Canada's policy requirements, do not result in downloading, printing or documentation of personal information. Interpreters trained in language interpretation are the only representatives who have access to personal information throughout the encounter. Access to personal information is granted after obtaining consent from the caller to engage third party interpretation services to facilitate the call in the caller's language of choice. Interpreters do not audio record or document details of the call.

2. Relay Health
In rare circumstances, Relay Health may be granted remote access from outside Canada when supporting local IT on a technical issue for resolution. Access is temporary and only utilized when local IT cannot resolve. To ensure the security of information, access is granted through a secure VPN. Policies and procedures dictate that at no time shall Relay Health download or copy information. As well, employees of Relay Health, under the umbrella of McKesson Corporation, are bound by the Corporate Code of Conduct.

3. McKesson Corporation, Secure Health Record (SHARE)
McKesson developers need to access the SHARE system from their offices, outside of Canada to deploy the software changes and test the upgrade software. No data is stored outside of the country.

McKesson's development staff will use a pre-existing secure 'data tunnel' to connect the McKesson test system to complete the upgrade testing. SHARE is located in the HITS-NS data center. All users accessing the data will require security sign-on and will need to be given access by the hospital IT staff.

Select McKesson developers/testers will have access to the test system. McKesson developers/testers will be pre-approved and must sign a confidentiality agreement. McKesson developers/testers access will be terminated immediately at test completion which occurred during fiscal year 2013-2014. No personal information will be downloaded or copied by McKesson. All requests into SHARE is tracked, and audit reports may be 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 for the protection of privacy of certain individually identifiable health information referred to as protected health information.

4. McKesson Corporation, Relay Health solution:
Personal Health Record (PHR) Pilot Project
In rare circumstances, Relay Health may be granted remote access from outside Canada when supporting local IT on a technical issue for resolution. Access is temporary and only utilized when

local IT cannot resolve. To ensure the security of information, access is granted through a secure VPN. Policies and procedures dictate that at no time shall Replay Health download or copy information. As well, employees of Relay Health, under the umbrella of McKesson Corporation, are bound by the Corporate Code of Conduct.

5. FairWarning
The Master Agreement with FairWarning prohibits storage or access of personal information outside of Canada unless the Department of Health and Wellness consents in writing.
FairWarning's development staff will use a pre-existing secure 'data tunnel' (VPN) to connect to the information stored on the appliance server to complete the configuration and testing of reports. The appliance server is located in the provincial data center.

Select FairWarning project managers/developers/testers will have access to the information. No personal information will be downloaded or copied by FairWarning. The FairWarning appliance keeps a log of all access to appliance / application. The vendor will also inform HITS-NS when they access the server to perform maintenance. Access logs will be reviewed for compliance. No patient data will be downloaded or copied from the appliance.

FairWarning Corporation is committed to following all Health Insurance Portability and Accountability Act ("HIPAA") regulations and all Ministry requirements for protecting patient information in Canada. HIPAA is United States federal law which includes provisions for the protection of privacy of certain individually identifiable health information referred to as protected health information.

6. DHW Employee Access:
The Department of Health and Wellness requires that personal information or personal health information not be sent via ensure unless encrypted via a secure file transfer protocol. This has been communicated through training, and will be reinforced though policy being developed during the 2014 calendar year. Therefore, the amount of personal information held or sent by e-mail, and therefore available for access while staffs were outside the country, should be limited. All BlackBerry devices and laptops issued by the Department are automatically password protected.

Reasons

1. Language Line Services – HealthLink 811
McKesson Canada has entered into a partnership with Language Line Services to meet contractual requirements for the provision of culturally safe care and improving access to primary health care services for all Nova Scotians. This third party interpretation service is required to address linguistic barriers. The interpreter service is provided over the phone.

2. Relay Health
McKesson Canada's subsidiary in the development of the Teletriage application is Relay Health. As a result, Relay Health is the only available provider of third level technical support for the information technology application that enables HealthLink811 operations.

3. McKesson Corporation, Secure Health Record (SHARE)
The McKesson product used for the provincial SHARE system is propriety to McKesson so no other vendor can perform the changes. The McKesson code and product development site is located

in the United States.

4. McKesson Corporation, Relay Health solution:
Personal Health Record (PHR) Pilot Project
McKesson Canada's subsidiary in the development of the PHR application is Relay Health. As a result, Relay Health is the only available provider of third level technical support for the information technology application that enables the PHR.

5. 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.

6. DHW Employee Access:
When staff are 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.

Intergovernmental Affairs

Description

Three employees of Intergovernmental Affairs took their Blackberries along with them on four trips outside of Canada. One employee took a Government laptop outside of Canada. These devices could have potentially contained personal information.

Conditions

Staff were briefed on the process for a lost or stolen Blackberry and those Blackberries are secured by CIO policy including password protection. The laptop was secured according to CIO standard with a password. No data was loaded onto the laptop other than the documents for use in meetings being held.

Reasons

These devices were necessary for travelling staff to continue to communicate and to continue to work and support the objectives of individual trips.

Innovacorp

Description

Eleven employees travelling for business or work to locations that include California, Brazil, Florida, New York, Georgia, Turks and Caicos, Massachusetts, Pennsylvania, Tennessee, Nevada, Maine, China. In addition, employees at the company use DropBox and DealFlow for transferring and storage of information.

Conditions

No unapproved use or disclosure by service providers.

Reasons

The storage and access of information is necessary due to the fact that the product or service is not available in Canada.

Justice

Description

1. Thirty two (32) employees traveled outside of country with a Blackberry or laptop that contained personal information or could access personal information.

2. In 2008 Correctional Services awarded JEMTEM Inc. the contract for Electronic Supervision of Offenders, the particulars about the decision can be found in the 2012 PIIDPA Report.

3. In 2005, the Emergency Management Office purchased an electronic information management system called eTeam from NC4 Corporation of California, USA that is installed and maintained on provincial government servers within the Provincial Government's Data Center. The technical support person in the US can remotely access the eTeam system to implement upgrades to the system. The particulars about the decision can be found in the 2012 PIIDPA Report.

4. Automon, Legal Services Practice Manager (PM) the vendor, can access the server to do Tier II application maintenance support to provide routine upgrade through a proxy remote access desktop session. The particulars about the decision can be found in the 2012 PIIDPA Report.

5. In July 2004, the Department of Justice entered into a service contract with Iron Mountain Canada Corporation to provide document destruction and government record storage. The particulars about the decision can be found in the 2012 PIIDPA Report.

6. The Director of MEP has an obligation, pursuant to the Maintenance Enforcement Act, to enforce all maintenance or support orders which have been filed for enforcement with the Director, including outside of Canada. The particulars about the authority and the decision for this obligation can be found in the 2012 PIIDPA Report.

Conditions

1. Employees are expected to maintain communication with staff at the office and ensure that their Blackberries and laptops are password protected and that the Government server is utilized.

2. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report.

3. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report.

4. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report.

5. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report.

6. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report.

Reasons

1. Permission to take Blackberry out of the country was granted to allow contact with staff and to deal with matters or urgent issues while travelling.

2. The particulars about how this service meets the necessary requirements of Justice's operations can be found in the 2012 PIIDPA Report.

3. The particulars about how this service meets the necessary requirements of Justice's operations can be found in the 2012 PIIDPA Report.

4. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report.

5. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report.

6. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report.

Labour and Advanced Education

Description

1. There were approximately ten (10) departmental employees who traveled outside Canada with a Blackberry electronic device with some contact information, for departmental operational purposes, who may have accessed personal information through email. None of the laptops, which were taken outside of Canada for departmental purposes, contained any personal information.

2. See description of access (or storage) provided in the 2012 annual PIIDPA report

Conditions

1. Authorization for traveling across international border with these electronic devices was authorized by the Deputy Minister in all cases in keeping with government policy and protocol.

2. See description of access (or storage) provided in the 2012 annual PIIDPA report

Reasons

1. When staff are travelling for business reasons, they are expected to monitor their email and voice mail for business continuity and operational purposes.

2. See description of access (or storage) provided in the 2012 annual PIIDPA report

Natural Resources

Description

1. Staff members who travelled outside Canada on business may have had the ability to access personal information via remote e-mail, Blackberry, personal computer or by other means.

2. Staff members who travelled outside Canada on pleasure may have had the ability to access personal information carried on e-mail or stored in Outlook via remote access to Outlook e-mail system.

3. Offside record storage was contracted with Iron Mountain Canada Corporation (subsidiary of the American Company).

Conditions

1. Remote access to Outlook is protected by username/password authentication, and is delivered over an SSL-encrypted link via the secure Blackberry Enterprise Server.

2. Remote access to Outlook is protected by username/password authentication, and is delivered over an SSL-encrypted link.

3. Iron Mountain is to safeguard and maintain protected storage of the department's records. Iron Mountain Canada Corporation confirms that personal information is maintained and disclosed in accordance with our contractual arrangement in compliance with all applicable privacy legislation.

Reasons

1. When staff are travelling for business reasons they are expected to monitor their e-mail and voice-mail for business continuity and operational purposes.

2. When staff are travelling for pleasure there may be times when they are required, or it is desirable for them to maintain contact for operational purposes.

3. Offsite storage of backup media/microfilm is required as part of the Disaster Recovery Program. The offsite storage is required to ensure vital records can be recovered should an incident occur.

Nova Scotia Business Inc.

Description

1. See description of access (or storage) provided in the 2012 annual PIIDPA report

Conditions

1. See description of access (or storage) provided in the 2012 annual PIIDPA report

Reasons

1. See description of access (or storage) provided in the 2012 annual PIIDPA report

Nova Scotia Liquor Commission

Description

No additional decisions were made during this calendar year to change the way the NSLC stores information outside of Canada. The current arrangement remains in place (see 2010 Annual PIIDPA Report).

Conditions

All data accessed outside of Canada is secure and encrypted (see 2010 Annual PIIDPA Report).

Reasons

Services that need to go outside of Canada for storage are assessed for benefit and cost. Any decisions that NSLC makes in this regard are reviewed with the legal team to ensure compliance and storage safety (see 2010 Annual PIIDPA Report).

Nova Scotia Utility and Review Board

Description

1. Off-site storage provided by foreign entity subsidiary

- **Payroll Service:** The Board continues to use the services of Ceridian Canada to process its payroll. Ceridian Canada is a subsidiary of Ceridian HCM Holding Inc., a US company.

2. Employee Access to Personal Information by Mobile Device

- **Employee Access to Personal Information by Mobile Device (Blackberry or Computer):** There were four instances where employees traveled outside of Canada with the ability to access personal information through a secure portal into the Board's internal network via mobile device or remote access.

Conditions

1. Off-site storage provided by foreign entity subsidiary

- **Payroll Service:** The service provider has agreed not to store information outside of Canada.

2. Employee Access to Personal Information by Mobile Device

- **Employee Access to Personal Information by Mobile Device (Blackberry or Computer:** Access to the Board's internal network is protected by username/password authentication and is delivered over a secure portal. Employees are required to use this portal when accessing personal information. Employees are also required to immediately report any theft or loss of the device or any suspected breach of information.

Reasons

1. Off-site storage provided by foreign entity subsidiary

- **Payroll Service:** No suitable compliant service provider has been found in Canada.

2. Employee Access to Personal Information by Mobile Device

- **Employee Access to Personal Information by Mobile Device (Blackberry or Computer:** When travelling, staff may be expected to monitor their email and voice mail for business continuity and to fulfill their job related responsibilities.

Premier's Office

Description

Two employees took their electronic devices outside the country with the permission of their Deputy Head.

Conditions

N/A

Reasons

In accordance with PIIDPA, the employees were permitted to take their electronic devices out of the country, to meet the requirements of the department's operation and / or the performance of their duties.

Public Prosecution Service

Description

Two employees traveled outside of Canada with their Blackberrys.

Conditions

The conditions placed on such access involved the use of encryption and password protection. Devices were in the custody of the person at all times.

Reasons

1. Access was necessary to check for work related messages. Messages received were responded to and staff given direction as required. Information was received from head office and responded to in a timely manner.

Public Service Commission

Description

1. Nine employees travelled outside Canada with a Blackberry mobile phone.

2. The department internet and intranet sites employ Google Analytics to monitor web site traffic. Google Analytics is a service provided by Google, based in the USA.

Conditions

1. The Blackberry devices were password protected and were used for work-related communication.

2. Google Analytics records the IP address of a user, provided by their Internet Service Provider, as they access the site. The IP address is masked to provide partial anonymity by removing the last portion of the IP address.

Reasons

1. The Blackberry was necessary to facilitate work related communication.

2. Analytical information allows the department to monitor use of the internet and intranet as a communication and support channel for government employees, and the wider population.

Securities Commission

Description

Remote access via Blackberry or other electronic device. There were 17 instances that staff members were approved to take their Blackberry or other electronic device while travelling outside Canada and may have accessed personal information.

Conditions

Permission must be granted in order to take a Blackberry or laptop out of the country. Remote access to email is protected by username/password authentication and is delivered over a secure server link (SSL) – encrypted link. All devices must be password protected.

Reasons

When staff travel, they may be required to conduct business or maintain contact with operations.

Service Nova Scotia and Municipal Relations

Description

1. Credit card transaction information resulting from payments for online services under the ACOL Contract or for in-person services delivered by SNSMR at Access Centres, Registry of Motor Vehicle Offices, Land Registration Offices, Alcohol and Gaming Offices, and the Business Registration Unit, or mail-in services is subject to trans-border data flow through United States 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.

2. Seventeen (17) SNSMR staff traveled outside Canada during the reporting period on twenty-six (26) separate occasions and took their laptop and/or Blackberry while away.

3. SNSMR currently stores 6219 boxes of records with Iron Mountain, a Canadian subsidiary of an American owned company which may be subject to the US Patriot Act.

4. SNSMR currently shares commercial vehicle and driver information with IFTA, Inc and the member jurisdictions in order for the province to be a member of the International Fuel Tax Agreement.

5. The Interprovincial Record Exchange Program is a system that allows Canadian motor vehicle jurisdictions to securely query other jurisdiction's driver and vehicle records. The Canadian Council of Motor Transport Administrators (CCMTA) acts as the clearing house and administrators for this system, and operates the secure network over which it runs. A partnership arrangement currently exists with the American Association of Motor Vehicle Administrators (AAMVA) to extend the system to the US.

6. The International Registration Plan (IRP) is an agreement among states of the US, the District of Columbia and provinces of Canada providing for payment of commercial motor carrier registration fees. As a participant in this plan the Registry of Motor Vehicles shares data with the IRP clearinghouse as well as non-clearinghouse jurisdictions that participate in the plan.

7. In 2006, MorphoTrust USA (formerly 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. 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 and continuing, Digimarc support technicians in Billerica, Massachusetts and Fort Wayne, Indiana have been 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 MorphoTrust USA 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.

Conditions

1. 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.

2. Remote access to GroupWise/Outlook is protected by Username/Password authentication and is delivered over an SSL-encrypted link.

3. Iron Mountain is under contract to maintain safe and private storage of the records in Canada.

4. All information is to be protected within the confines of the agreement with IFTA, Inc. and only shared with member jurisdictions and our service provider, Xerox Canada Inc.

5. CCMTA acts as the clearing house for all queries so that jurisdictions do not have direct read access to another jurisdiction's system. Queries are forwarded to/from member jurisdictions only (CCMTA & AAMVA). Queries are pre-formatted and specific as to what information is displayed. CCMTA has contracts with each of its member jurisdictions that conform to the jurisdiction's privacy legislation concerning disclosure and consent.

6. The data is shared as per the agreement without restriction.

7. 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.

Reasons

1. SNSMR offers credit card payments as a convenience for customers and to provide efficient and effective online services to clients.

2. Maintain contact with operations.

3. The Provincial Records Centre used to store their records overflow at Iron Mountain in the mid to late 1990s. In 1997 the Iron Mountain accounts created by the Provincial Records Centre were transferred to the various departments who had overflow records stored with Iron Mountain. At this time, SNSMR took over ownership of the Iron Mountain relationship. The Provincial Records Centre will not currently accept any records from SNSMR that are not backed by STOR and until the STOR has been developed and SNSMR can find the appropriate funding to transfer the records out of Iron Mountain, SNSMR is forced to use commercial storage facilities due to space restrictions within their operating offices.

4. It is an operational requirement to be a member of the International Fuel Tax Agreement. IFTA provides a system where its members share fuel tax revenues. Under this agreement, licensees file a fuel tax return quarterly to their base jurisdiction indicating the amount of fuel purchased and kilometres travelled. The base jurisdiction then verifies how much fuel tax was paid in each jurisdiction and how much tax is owed to each jurisdiction. The base jurisdiction assesses the licensee for any outstanding balance owing and sends a monthly return to each affected jurisdiction to cover the net balance. In addition, the IFTA system and data are stored and maintained in Tarrytown, New York by our vendor, Xerox Canada Inc. As part of the annual IFTA application process, Nova Scotia IFTA applicants consent to their data being shared with IFTA, Inc., the member jurisdictions and a service provider contracted to provide data services.

5. 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.

6. This agreement has been in place since 1999 with security measures in place since then. In fiscal year 2013/14 it was confirmed that only IRP jurisdictional staff have access to this information which is password protected on a secure web site.

7. Access by MorphoTrust USA (formerly 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.

Transportation and Infrastructure Renewal

Description

Forty-three (43) employees were approved to access their wireless devices when travelling outside Canada while on business or pleasure (see same description for reason of access in 2012's annual PIIDPA report).

Conditions

See same description for conditions of access in 2012's annual PIIDPA report.

Reasons

See same description for reason for access in 2012's annual PIIDPA report.

Workers' Compensation and Appeals Tribunal

Description

There was no storage of personal information in the custody or control of the Tribunal outside of Canada from January 1, 2013, to December 31, 2013. Approximately six employees traveled outside of Canada for pleasure with the ability to access personal information carried on e-mail or stored in the GroupWise or Microsoft Outlook e-mail system via remote access using personal electronic devices or computers outside of Canada.

Conditions

Remote access to staff e-mail accounts through web access to GroupWise or Outlook is protected by user name/password authentication.

Reasons

Staff travelling out of the country, on occasion, monitor their e-mail account for operational requirements to ensure that any urgent matters are dealt with appropriately. They do not conduct business nor access any personal information but simply refer matters for disposition.

Workers' Compensation Board of Nova Scotia

Description

1. Employee access to personal information by mobile device (iPhone, iPad, Blackberry) or computer (laptop, desktop)

Thirty-five (35) instances of employee travel outside of Canada with the ability to access personal information through a secure portal into the WCB's internal network via mobile device or remote access.

2. Employee access to personal information by remote access only

1,124 individual's personal information (contained in unique claim files) accessed from a remote location outside of Canada (in the US) through a secure portal into the WCB's internal network by remote access.

3. Medical Consultant access to personal information

Twenty-seven (27) individual's personal information (contained in unique claim files) accessed from a remote location outside of Canada (in the US) through a secure portal into the WCB's internal network by remote access.

4. Translation Services

Fifty-six (56) instances of personal information were accessed by translation services procured by Language Line Services. Language Line Services was contracted to provide telephone based language interpreter services for callers whose first language is not English. Language interpreters may be located in any one of a number of countries in or outside North America. Calls involving interpreters are not audio recorded nor do the interpreters document any details of the call; therefore no recorded information is collected or stored outside of Canada.

Conditions

1. Employee access to personal information by mobile device (iPhone, iPad, Blackberry)

Access to WCB's internal network is protected by username/password authentication, and is delivered over a secure portal. Immediate report of theft/loss of device or information is required.

2. Employee access to personal information by remote access

Access to WCB's internal network is protected by username/password authentication, and is

delivered over a secure portal. Immediate report of theft/loss of device or information is required.

3. Medical Consultant access to personal information

Access to WCB's internal network is protected by username/password authentication, and is delivered over a secure portal. Information limited to only necessary medical information required to complete a review and provide medical report.

4. Translation Services

Language Line obtains a signed confidentiality agreement from each respective interpreter and reviews these agreements once annually. The interpreter service is provided over the phone. Language Line Services does not result in downloading, printing or documentation of personal information. Interpreters trained in language interpretation are the only representatives who have access to personal information throughout the encounter. Access to personal information is granted to Language Line after the WCB obtains the consent from the individual to engage third party interpretation services to facilitate the call in the caller's language of choice. Interpreters do not audio record or document details of the call.

Reasons

1. Employee access to personal information by mobile device (iPhone, iPad, Blackberry), computer (laptop, desktop)

When staff travel for business or personal purposes and they are expected to monitor their email and voicemail for business continuity, and to fulfill their job related responsibilities, they must abide by the restrictions noted above.

2. Employee access to personal information by remote access

When staff travels for business or personal purposes they are expected to monitor their email and voicemail for business continuity, and to fulfill their job related responsibilities, they must abide by the restrictions noted above.

3. Medical Consultant access to personal information

Medical consultant specializes in both occupational and environmental medicine, providing unique capabilities required in the interest of allowing the WCB to administer the *Workers' Compensation Act, Regulations* and Policy.

4. Translation Services

This third party interpretation service is required to address linguistic barriers associated with service delivery in the interest of allowing the WCB to administer the *Workers' Compensation Act, Regulations* and Policy. The interpreter service is provided over the phone.

District Health Authorities

Annapolis Valley District Health Authority

Description

Approximately eight (8) AVDHA employees travelled outside of Canada and may have accessed their Blackberry, laptop or other electronic device containing personal health information. No new service contracts were entered into that allowed or required access or storage of personal information outside of Canada.

Conditions

See description of restrictions or conditions placed on storage or access outside Canada provided in the 2012 annual PIIDPA report

Reasons

See statement provided in the 2012 annual PIIDPA report.

Cape Breton District Health Authority

Description

1. A total of eleven (11) employees travelled outside Canada and may have accessed email with their Blackberrys or notebooks.

2. Application Support Contracts for software or systems with possible access to personal information. See description of access or storage provided in the 2012 annual PIIDPA report.

Conditions

1. N/A

2. All new and renewed contracts have inclusion clauses requiring vendors to comply with PIIDPA legislation.

Reasons

1. N/A

2. Current access to and storage of information outside of Canada is linked to pre-existing programs and/or systems utilized in CBDHA and deemed necessary for ongoing operations.

Capital District Health Authority

Description

1. Vendors requiring access to personal information from outside of Canada are granted access on a need to know basis for the purpose of equipment and IT system maintenance, as necessary for the operations of the health authority and when the expertise does not exist in house.

2. Staff members travelling outside of Canada may have accessed personal information via remote access or their blackberry.

Conditions

1. PIIDPA compliance is a requirement in all new and renewed contracts where there is the potential for storage or access of information outside of Canada. CDHA's Privacy Policy also applies.

2. Staff seeking remote access must apply for privileges and their equipment must have the required security controls, as per the CDHA Remote Access Policy.

Reasons

1. Current access to and storage of information outside of Canada is tied to pre-existing CDHA programs and/or systems that are necessary for operations.

2. Staff members who are travelling may require access to personal information for the following purposes: patient care, business continuity and operational support.

Colchester East Hants Health Authority

Description

1. CEHHA had no staff member that travelled outside of the country that accessed personal information during the 2013 calendar year.

2. Vendors requiring access to personal information from outside of Canada are granted access on a need to know basis for the purpose of equipment and IT system maintenance as necessary for the operations of health authority and when the expertise does not exist in house.

Conditions

2. Contracts: All new and renewed contracts have inclusion clauses requiring vendors to comply with PIIDPA legislation.

Reasons

2. Contracts: Current access to and storage of information outside of Canada in linked to pre-existing programs and/or systems utilized in the Colchester East Hants Health Authority and deemed necessary for ongoing operations.

Cumberland Health Authority

Description

1. Decision was made to provide the following (including, but not limited to):

- VPN access to Dictaphone System from Florida, US offices for remote vendor application support.
- Encrypted (SSL) staff access to CHA web mail system from US locations.
- Storage of information on whole disk encrypted DHA owned laptops.
- Access to email using Blackberry mobile devices.

2. Decisions regarding storage/access of personal information outside of Canada are pending upon future guidance, regulations, policies and procedures.

Conditions

1. Access to information stored on CHA networks and servers is only permitted through encrypted VPN connections. All external email access is encrypted through SSL, VPN (IPSEC) or the Blackberry service. The CHA 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 US storage devices and CD/DVD's. Blackberry devices have been secured with passwords and auto-wipe features.

2. 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.

Reasons

1. Access and storage from outside of Canada is linked to pre-existing programs and/or systems utilized in the Cumberland Health Authority and are deemed necessary in the ongoing operations of these systems and programs.

Guysborough Antigonish Strait Health Authority

Description

1. There were no decisions made to allow storage or access outside Canada.

2. There were about five (5) staff members who travelled outside of Canada with their Blackberry devices.

Conditions

2. Existing systems are managed by IT support in HITS-NS or Cumberland Health Authority with VPN. VPN access is necessary for software maintenance and/or product support. Blackberry devices are password protected. Laptops or USBs containing confidential information are encrypted.

Reasons

2. The staff may not have accessed personal information, however, any access would be deemed necessary as part of employment obligations.

IWK Health Centre

Description

1. Laboratory Testing IWK contracts with laboratories outside of Canada if specialized testing services are not offered in Canada, or if the cost of having the required tests performed in Canada is prohibitively high. IWK seeks referral laboratories in the USA first, and if the required testing is unavailable or inappropriate, IWK seeks referral labs in Europe or Australia. In accordance with the IWK Department of Pathology and Laboratory Medicine policy, efforts are made to work only with referral laboratories that meet international standards with respect to the collection of information, collection of samples, and storage and retention of medical records. During the 2013 calendar year, IWK worked with 114 international referral testing facilities, 80 laboratories in the USA and 34 international laboratories (13 laboratories in Germany, 9 laboratories in the United Kingdom, 5 laboratories in the Netherlands, 4 laboratories in Belgium, and 1 laboratory in each of Estonia, France and Australia).

2. Non-Canadian Contractors/Vendors with Remote Access IWK contracts with some specialized service providers who, in the course of providing their services, access remotely or store outside of Canada, personal information in the custody and control of IWK. IWK's IT department facilitates the access, and HITS Nova Scotia provides VPN software on service providers' systems (all information accessed remotely is done via the encrypted HITS-NS Aventail VPN solution). When dealing with large vendors, Site-to-Site VPN access can be used. Terms of access are contractually controlled. Examples of key IWK service providers who may store or access personal information outside of Canada include: Meditech: Boston, Massachusetts, USA (IWK patient information system); Agfa: Wilmington, Massachusetts, USA (medical imaging equipment and supplies); Pyxis: San Diego, California, USA (medical safety systems and technology); EMC Corporation: Hopkinton, Massachusetts, USA (healthcare data and information sharing services and technology); Blackbaud: Charleston, South Carolina, USA (non-profit management/accounting software); Genial Genetics: United Kingdom (laboratory software for genetic data management); Innovian: Germany and USA (IWK anesthesia system); Maximo Corporation: Irvine, California USA (support for clinical monitors in Medical Surgical and Neuroscience Unit and Pediatric Medical Unit); Alere Infomatics: Tampa, Florida, USA (support for glucose meter management system); and GE Healthcare: United Kingdom (ultrasound system).

3. Business Travel: IWK's records indicate that during the 2013 calendar year there were 183 incidents of travel booked through the IWK for work-related travel outside of Canada, by 155 IWK staff members. Staff members do not usually require access to personal information in the IWK's custody and control during international business travel; accordingly, personal information may not have been stored or accessed outside of Canada during these incidents of international travel. Further, mobile devices, including laptops and cell phones, are generally only used for e-mail and/or telephone access while staff are traveling internationally and are not typically used to transport or access personal information.

Conditions

1. Laboratory Testing Consent is obtained from patients wherever practicable prior to sending samples to be tested at laboratories outside of Canada. IWK Laboratory Services carefully tracks all external referrals, whether sent inside and outside of Canada. The Department of Pathology and Laboratory Medicine has a Laboratory Standards Coordinator, responsible for monitoring referral laboratories for current accreditation and licensing/certification status, in accordance with the Department's Evaluation, Selection and Monitoring of Referral Laboratories Policy. New referral labs, and new testing sent to current labs, are submitted to the Laboratory Standards Coordinator for an assessment application process, and information regarding all assessed laboratories is maintained in an IWK laboratory database. The accountability for the non-Canadian laboratories selected lies with the IWK Clinical Division Head, Pathology and Laboratory Medicine. All laboratories are checked every 6 months for current accreditation status.

2. Non-Canadian Contractors/Vendors with Remote Access: When IWK contracts with service providers where there is potential for storage of or access to personal information outside Canada, then wherever practicable, IWK obtains individuals' consents or uses contractual conditions to protect privacy and confidentiality (including requiring vendors to agree to secure network access requirements, confidentiality clauses, and other accountability measures intended to safeguard personal information). IWK's Privacy Office oversees standard remote access given to vendors, and requires vendors to complete remote access forms to allow IWK to appropriately limit and control the type of access. In addition, 'Privacy Impact Assessments' (PIAs) are completed for any new service at IWK which involves the access or storage of personal information outside of Canada. The PIA is reviewed by the IWK Privacy Officer to ensure that risks of disclosure of personal information are properly addressed and mitigated. An example of a non-Canadian service provider web-based surveying tool sometimes used by IWK is Survey Monkey. Survey Monkey's server is located outside of Canada (therefore, so is any data input into the tool). As such, access to this tool is restricted on IWK's network. Alternative survey software which stores data on the local network, is available to IWK employees and physicians. The restricted access to Survey Monkey was implemented and the reasons for it communicated to IWK employees and physicians on May 1, 2009. Access remains restricted to-date, and authorization from the Privacy Office is required to access this tool on the network.

3. Business Travel: IWK staff members who require access to personal information in the custody or control of the IWK during international business travel are able to access the IWK's information systems using secure remote access connections. The staff member logs in to the system through protected remote desktop sessions/terminal services which connect directly to the staff member's IWK computer. All IWK issued laptops and handheld electronic devices have encryption software or are password protected. These measures protect the information on the device from unauthorized access or disclosure. Staff are also advised to configure their handheld devices so that e-mail is not accessible, while still allowing the telephone capabilities of the device to be used. In addition, the following restrictions and conditions have been placed on storage and access of personal information from outside of Canada: 'Active Directory' software protections are in place for

Terminal Servers and Remote Desktop Stations, which software allow IWK network administrators to control what users can do when accessing the IWK network remotely. For example, certain functions are controlled or prevented: copy/paste, remote printing and mapping of serial and printer ports. This software has the effect of turning a remote access session into a 'window' capable of viewing IWK systems, while preventing information from being removed from the system. IWK blackberries and staff phones are mandatorily password protected. Non-use of the device for five minutes will trigger the requirement to enter the password to unlock the device. If a user fails to enter the correct password in a set number of attempts, the device is automatically wiped of its data/content. IWK laptops have been and are being updated with encryption software to safeguard information stored on any lost, stolen or improperly accessed laptops, including USB portable memory drives used in those laptops.

Reasons

1. Laboratory Testing: Obtaining certain specialized laboratory testing services from outside Canada is necessary for IWK's operations, as the IWK provides genetic testing for the Maritime Provinces. Genetic testing is an evolving field continually requiring increasingly esoteric testing.

2. Non-Canadian Contractors/Vendors with Remote Access: The vendors IWK contracts with that store or remotely access personal information from outside Canada do so to deliver their specialized services. In many cases these vendors are the only companies providing service or maintenance for the products IWK requires and uses in its day to day operations, including specialized software and equipment.

3. Business Travel: International business travel may not involve the storage or access of personal information outside of Canada. However, in the event such access/storage does occur, it is generally for the purpose of ongoing patient care or an ongoing healthcare research project.

Pictou County Health Authority

Description

One release of information request in which the patient wanted personal health information (DI related) sent to a physician in Mexico. Verbal consent was received from the patient to send the information out of the country.

Conditions

Staff are not allowed to use their cellular devices out of the country without prior approval. Staff only used HIT-NS and PCHA approved electronic storage for all electronic information.

Reasons

With regards to release of information, consent of the patient must be attained. PCHA does not store any electronic information on servers outside of the country. If a request was attained, it would go through a review process to determine the risk and whether or not it is the only viable option for storage.

South Shore District Health Authority

Description

Between January 1, 2013, and December 31, 2013, there were two (2) South Shore Health employees who travelled outside Canada who had the ability to access personal information from their blackberry devices. Both employees had approval from the CEO.

Conditions

Policies exist covering restrictions. Blackberry devices are password protected and also have an auto wipe feature.

Reasons

Policies exist covering restrictions on blackberry devices.

South West District Health Authority

Description

1. In 2013, there were 13 employees involved in international trips where they maintained access to the organization through Blackberries, remotely through VPN or through the nshealth.ca web network. All staff members reported that they maintained contact for organizational reasons.

2. In 2013, SWH entered into service agreements with the following vendors/instruments/models:

Lab:

- Fisher Scientific – Tissue Embedding Centre/Microtome with blade holder
- Radiometer – ABL825/ABL5
- Somagen Diagnostics – Tissue Processer.
- Siemens – Clinitek 500/Clinitek Atlas

DI:

- BCL Xray Canada – GE Portable PMX/QMI NX/DR/ATL Ultrasound/GE General X-ray/LOGICQ9/DMD Logar/GE Mobile AMX/QMI General/Sedecal mobile
- GE Healthcare – Logiqu E 9/DT
- Siemens Canada – SPECT/CT GAMMA Camera

OR:

- Alcon Canada Inc.
- Carl Zeiss Canada
- GE Healthcare – Anesthesia Equipment

Pharmacy:

- Omnicell Inc.
- Healthmark Ltd.

Respiratory:

- Cardinal Health Canada

Health Records:

- Nuance Communications

Conditions

2. The district continues to add the inclusion clause re: the management of the information in all requests for proposals, new contracts, warranties or renewals. All SWNDHA vendor contracts include language meeting the regulatory requirements from the PIIDPA legislation as part of the agreement. The vendor must abide by the Act and any other applicable Act or regulation that pertains to disclosure of patient information.

Reasons

2. SWH uses software vendors located outside Canada who maintain systems remotely; for example: Meditech (Health Information); SAP (financial and personal); Nuance (transcription/dictation); and Siemens (DI equipment). Again, the access to systems are managed by written agreements and monitored by SWH.

Specialized lab testing either unavailable in Canada or cost prohibitively in Canada are sent outside the country.

Universities

Cape Breton University[2]

Description

1. Alumni / Donor database: CBU uses software provided by an American vendor, Blackbaud, located in South Carolina. Although the system originates from the US, data on university alumni and donors is housed on servers at the CBU campus. Blackbaud does provide remote technical service. If authorized by the university, it is possible for a Blackbaud technician to access the CBU system under CBU supervision.

2. Student Information System: CBU Faculty may access portions of the CBU Student Information System when out of the country for the purposes of viewing the records of students in their respective courses and entering term grades. This could be the result of a faculty being out of the country during the period of time grades are submitted, or by a faculty teaching program. As well, 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 enrolled in the courses.

4. Residence Management: CBU is in the process of implementing StarRez, a Residence Management System provided though StarRez Inc. from Greenwood Village, Colorado. During implementation, and as it becomes operational, all data is stored and secured in the CBU Data Centre. Access to the system by StarRez employees is for troubleshooting only and is supervised by a CBU employee.

5. SharePoint: Various groups on campus use SharePoint for collaboration and data storage. While all data is secured in the CBU Data Centre, web access is available to these sites for authorized users.

6. Approximately 50 members of the CBU facility and staff have travelled outside Canada in 2013 with web access to the personal email via smart phone, tablet or laptop. Some would also have

[2] Acadia University, Atlantic School of Theology, Mount St. Vincent University, NSCAD had no access or storage outside of Canada to report.

access to the Student Information System and/or various SharePoint sites. 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.

Conditions

Access to personal information outside Canada is limited to authorized personnel. In the case of an external entity requiring access for the purpose of trouble shooting a particular system, all access is controlled, time restricted, and done under the supervision of CBU staff.

Reasons

For the Alumni / Donor database, and the StarRez system, these American developed products were determined to be the best fit for CBU needs, and are widely used in Canada. Access by these forms is restricted as described above. With respect to access by CBU employees traveling outside the country, such access is necessary for university administrators, reserchers, and other employees to perform their assigned duties.

Conseil Scolaire Acadien Provincial

Description

1. A number of employees traveling outside Canada for business or for pleasure.

2. The board approved eight school trips outside Canada for a variety of learning experiences.

3. The board has online subscriptions for education media Learning A to Z.

4. KEV Group is an international company that specializes in the management of school activity funds.

5. SAP is an internal enterprise resource planning system used for finance, human resources and procurement.

6. The Provincial Student Information System (SIS) is used to manage school operations. TIENET is a component of SIS and is used to manage the student documentation associated with the Program Planning Process.

Conditions

1. Email accounts and remote storage areas are accessible by username and password authentication. Access to devices (laptop / tablet / intelligent phone / external hard drive / memory stick) are to be password protected.

2. Personal information contains parents / guardian contact and student health information (i.e., allergies and medication requirements).

3. Requirements for the subscription: teacher's name and school name.

4. Accessed by KEV employees only where required for maintenance and troubleshooting.

5. See details provided in the 2012 NS annual PIIDPA report under Finance.

6. See details provided in the 2012 NS annual PIIDPA report under Education.

Reasons

1. Executive members are required to monitor mail using intelligent phones to allow contact with staff members to deal with urgent matters. Staff members may be required to prepare documents and access internet sites for business continuity purposes and maintain contact with operations using communication devices.

2. Staff members accompanying students are required to have in their possession or the ability to rapidly access this type of personal information in case of emergencies while away.

3. No Canadian alternatives identified.

4. SchoolCash was the only product that provided the required language and functionality at a price advantage offered by Canadian vendors.

5. See details provided in the 2012 NS annual PIIDPA report under Finance.

6. See details provided in the 2012 NS annual PIIDPA report under Education.

Dalhousie University

Description

1. Online Communications and Collaboration Tools. International storage of online collaboration and communication tools, including email and calendar services, provided to employees, students and alumni (email only). Primary data centre located in the United States.

2. Academic Instructional Tools. Academic instructional tool, which enables instructors to build and implement electronic assignments and activities. Data stored in United Kingdom.

3. Athletics Schedules and Scores. Program used to manage athletic season schedules, rosters and scoreboard results. Data stored in United States.

4. College Student Inventory (CSI). A student assessment tool which identifies the individual strengths and challenges for each member of an incoming class, as well as their receptivity to our interventions, early in the first term. This student assessment provides data to make interventions more meaningful and relevant, before a student has made a decision to stay or leave. With the CSI, you prioritize your interventions more effectively, connect at-risk students to the resources they need most, and help more of your incoming students persist. The CSI module is part of an early-alert retention management system, being a comprehensive suite of student success assessments and analytics that help identify which individual undergraduates are most at risk, gauge students' receptivity to assistance, connect at-risk students to the most appropriate campus resources, and design or fine-tune appropriate support services. This system also gives detailed summary data on the needs of student cohorts, making it easier to help groups of students complete their educational goals.

5. See descriptions of access and storage provided in the 2012 annual PIIDPA report for each of the following items: Financial Services Electronic Forms; University ID Card; Network and Systems Upgrades; Wireless Products; Apple Warranty Maintenance; Teaching and Research Statistical Software; Collaborative Teaching Software; Service Provider Maintenance (IBM Hardware and Software); Administrative Computing Software; Room Reservations Software; Degree Progress Software; Student Advising Scheduling Software; Student Performance and Referral Software; Medical Education Evaluations Software; Dentistry Academic Materials Software; Service Provider Maintenance (Xerox Hardware and Software); Website Feedback; Plagiarism Detection; Clinical Experience Software; Law Student Survey; Undergraduate Student Survey; Crowd Sourcing Product; Hosted Learning Management System; Student Learning Outcomes Software; Environmental Health & Safety Database; and Online Law School Exams.

6. Employee Temporary Remote Access. See description of access provided in the 2006 annual PIIDPA report.

Conditions

1. Online Communications and Collaboration Tools. Contractual obligations on service provider to not use or disclose data for other purposes, to maintain appropriate security measures to protect the data from accidental loss, destruction, alteration, or unauthorized disclosure, use or access, and to comply with applicable privacy laws. Developed internal exit strategy; Have alternative on-site services for sensitive data and will be looking to expand additional options. Ongoing development of best practice guidelines, education, training and communication to users.

2. Academic Instructional Tools. Use of the service requires authenticated access either through the learning management system integration or LDAP. The new data centre has achieved widely-adopted global security standard certification which covers infrastructure, data centers, and services, and sets out requirements and best practices for a systemic approach to managing company and customer information that's based on periodic risk assessments. Contract with service provider contains protection requirements, including obligation to use reasonable security measures to protect data against unauthorized access, use, disclosure and destruction, limited access by employees, return or destruction upon completion of services, prior notification of requests by foreign entities.

3. Athletics Schedules and Scores. Contractual obligations on service provider to take precautions to protect the data, to maintain confidentiality of the data and not use, distribute or disclose the data for unauthorized purposes.

4. College Student Inventory (CSI). This online service is protected by VeriSign Secure Site. All information sent to this site, if in an SSL session, is encrypted, protecting against disclosure to third parties. Service provider has signed a Non-Disclosure Agreement with Dalhousie which addresses issues relating to access, retention and storage of personal information. In particular, once personal information has been downloaded from the service provider's site, service provider only retains aggregated, non-identifiable data. Student Accessibility Services will download the personal information from service provider on a regular basis to ensure that identifiable information is stored on their database for a limited period of time. Service provider is also required to inform Dalhousie of any foreign demands for access to the personal information.

5. See descriptions of access and storage provided in the 2012 annual PIIDPA report for each of the following items: Financial Services Electronic Forms; University ID Card; Network and Systems Upgrades; Wireless Products; Apple Warranty Maintenance; Teaching and Research Statistical Software; Collaborative Teaching Software; Service Provider Maintenance (IBM Hardware and Software); Administrative Computing Software; Room Reservations Software; Degree Progress Software; Student Advising Scheduling Software; Student Performance and Referral Software; Medical Education Evaluations Software; Dentistry Academic Materials Software; Service Provider Maintenance (Xerox Hardware and Software); Website Feedback; Plagiarism Detection; Clinical Experience Software; Law Student Survey; Undergraduate Student Survey; Crowd

Sourcing Product; Hosted Learning Management System; Student Learning Outcomes Software; Environmental Health & Safety Database; and Online Law School Exams.

6. Employee Temporary Remote Access. See description of access provided in the 2006 annual PIIDPA report.

Reasons

1. Online Communications and Collaboration Tools. Email and calendar tools are essential aspects of the University's information technology services. They are key to the successful and efficient operation of the University, and form a necessary part of our learning and teaching, research and administrative processes. They are used extensively by members of the Dalhousie community to communicate and collaborate among themselves, and with third parties. The other collaboration and communications tools provide additional capabilities for students and employees to collaborate in creating and sharing work products such as documents, and offer a variety of means to communicate and collaborate among themselves, and with third parties. These tools are important aspects of the University's information technology services. They improve the effectiveness and efficiency of University business operations, our teaching, research and administrative processes, and student learning experiences. The option to continue to host these services in-house does exist, but at considerable cost and resources by Dalhousie to keep the services secure and up-to-date. There are also a number of shortcomings with the current in-house services, including limited functionality and ease of use, limited capacity, unreliability, limited security. Outsourcing the service to a cloud-based solution has numerous advantages as compared to in-house services, including enhanced security measures, greater service standards and reliability, improved functionality, increased storage capacity and cost savings. There are no comparable cloud-based solutions that store or access the data exclusively in Canada. Of all other cloud-based service providers, this service is superior in terms of functionality, security, service standards, reliability, compatibility with current computing systems, and cost. The hosting environment offers extensive processing and storage capacity with robust backup and failover capabilities, and superior operational and security controls. The service also offers superior integration capabilities with other products already in use at Dalhousie. In total, this service is a reliable, modern, industry-leading service that integrates well with Dalhousie's technical environment and offers significant economic advantage when compared to other services or an in-house system.

2. Academic Instructional Tools. This service has been in place for a few years for use in classroom and online instruction to enhance the educational experience of our students, and is fully integrated with our learning management system. The service provider made a company-wide decision to move from the Canadian-hosted data centre to an international data centre for enhanced security features. This is the only suite of products that has access control and integration with our existing learning management system. The service is part of the teaching curriculum and a switch to a new product during the academic term would be disruptive to students and faculty.

3. Athletics Schedules and Scores. Beneficial service as it eliminates post game statistics reporting, development of 200 player profile pages on internal website, and provide a schedule and scoreboard functionality for team website that isn't available in Dalhousie's suite of web components. Provides live statistics, schedule, scoreboard, roster and player profile functionality that is automatically linked in the system we are required to use by the national governing body of university sports. There is no other service that can match what this service provides given that it offers the in-game statistics function that is automated with uploading to the regional and national sports database, and provides schedule statistics, roster and player profile and scoreboard functionality to the regional and national governing bodies of university sports.

4. College Student Inventory (CSI). As a part of Dalhousie's core strategy and retention initiative, the CSI survey will be crucial to helping us identify individual strengths and challenges for our incoming Bachelor of Arts (BA) and Bachelor of Science (BSc) undergraduate students. Participation in the survey is voluntary. The CSI identifies the leading cognitive and affective indicators of students' success. Completed surveys will result in a detailed report with information about the student's academic motivations, levels of personal support, and receptivity to assistance. This information will help us to create a connection with incoming BA and BSc students during their first term. Engage students in reflective discussions about how to develop their talents and overcome areas of challenge. Match at-risk students to the services they need. This assessment also provides us with data to make our interventions more meaningful and relevant, before a student has made a decision to stay or leave. With the CSI, we will be able to prioritize our interventions more effectively, connect at-risk students to the resources they need most, and help more of our incoming students persist; superior than other products in terms of cost and functionality (can customize by adding our own questions, can be charged only for completed surveys, and can offer a mid-year assessment which will help us, among other things, measure changes in motivation, the campus services students utilize the most, and learn more about the services they request.

5. See descriptions of access and storage provided in the 2012 annual PIIDPA report for each of the following items: Financial Services Electronic Forms; University ID Card; Network and Systems Upgrades; Wireless Products; Apple Warranty Maintenance; Teaching and Research Statistical Software; Collaborative Teaching Software; Service Provider Maintenance (IBM Hardware and Software); Administrative Computing Software; Room Reservations Software; Degree Progress Software; Student Advising Scheduling Software; Student Performance and Referral Software; Medical Education Evaluations Software; Dentistry Academic Materials Software; Service Provider Maintenance (Xerox Hardware and Software); Website Feedback; Plagiarism Detection; Clinical Experience Software; Law Student Survey; Undergraduate Student Survey; Crowd Sourcing Product; Hosted Learning Management System; Student Learning Outcomes Software; Environmental Health & Safety Database; and Online Law School Exams.

6. Employee Temporary Remote Access. See description of access provided in the 2006 annual PIIDPA report.

Nova Scotia Community College

Description

1. The Nova Scotia Community College has allowed for the storage of personal information under our control to be held by Hobsons EMT (formerly Apply Yourself, Inc.). This company is located in Fairfax, Virginia in the United States. Hobsons EMT is an application service provider offering web-based data management for the College's on-line application process. The College has been using the services of Hobsons EMT effective March 21, 2005, prior to the Assent of the Act on July 14, 2006. Since our last submission (March 4, 2013), we investigated service providers within Canada, however, there were no emerging or known Canadian companies identified by us through the usual channels, conferences, trade shows and vendor contacts. The College is currently in the process of actively moving the on-line application process in house to our PeopleSoft ERP and will be launching this in Spring/Summer 2014. In the meantime, 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.

2. In 2012, the College implemented a Status Solutions LLC. life safety project (Situational Awareness and Response Assistant). Status Solutions LLC. is headquartered in Charlottesville, Virginia in the United States. The installation for the College is locally hosted and maintained in Nova Scotia. However, consultants located in Ohio in the United States were accessing information while assisting with the system setup and configuration. Access is provided in a secure manner and was specifically limited to the life safety project. No data was sent outside of Canada. Access to the system was rescinded upon completion of the project in 2013.

3. As required by the Act, the College will allow our employees to transport personal information temporarily outside Canada but only to the extent that it is strictly necessary for their assigned duties or as a necessary part of a research project. We anticipate that this information will be transported using cellular telephones, wireless handhelds, laptops and storage devices. In such event, employees will be required to take all reasonable precautions (e.g. encryption) to protect the personal information. For accessing personal information in College data repositories from outside Canada; the College will permit its employees and students to use web-based or other internet access tools if it is a necessary part of performing his or her assigned duties or as a necessary part of a research project. The College has seen increased usage of Dropbox and other cloud offerings on our networks. The College doesn't promote its usage but it can't stop it. The College is in the early planning stages to provide a secure local based service as an alternative.

Conditions

Contained within Descriptions provided above.

Reasons

Contained within Descriptions provided above.

St. Francis Xavier

Description

1. See description of access (or storage) provided in the 2012 annual PIIDPA report.

Conditions

1. See description of access (or storage) provided in the 2012 annual PIIDPA report.

Reasons

1. See description of access (or storage) provided in the 2012 annual PIIDPA report.

St. Mary's University

Description

1. **Plagiarism Detection:** See description of access or storage provided in the 2012 annual PIIDPA report.

2. **Maintenance Management System:** See description of access or storage provided in the 2012 annual PIIDPA report.

3. **Travel:** See description of access or storage provided in the 2012 annual PIIDPA report.

4. **Facilities Asset Management System:** See description of access or storage provided in the 2012 annual PIIDPA report.

5. **National Survey of Student Engagement:** Survey of 1st and 4th year undergraduate students.

6. **Schwab Charitable:** This US organization based in San Francisco, CA represents a private donor in the US who has established the Cole Harbour High Scholarship, an external award that provides tuition funding to students. Saint Mary's University does not have charitable status in the US but information is provided to show we are the equivalent of a charity by IRS standards. This year Schwab Charitable required the home addresses, telephone and birth days for all of the University's Board of Governors as part of their due diligence required for the transfer of funds to international charities.

7. **Software Update:** Management software for all aspects of our residence operation from room assignments to student billing to summer conference operations to incident management.

8. **Ruffalo Cody:** provides hosted, cloud-based call centre software to SMU, Development Office. Data is stored on Canadian Servers under industry-standard security protocols. Occasionally, for the purpose of troubleshooting and installation, data is accessed by our account manager located in the US. This data is accessed via a Canadian FTP server.

Conditions

1 through 4, see 2012 Annual PIIDPA report.

5. Indiana University is given names and email addresses of all 1st and 4th year undergraduates to facilitate promotion of participation in the survey.

6. All information stored on a secure dedicated server at SMU. Restricted remote access to update under the supervision of in-house technical staff.

7. Per Service Agreement with the Vendor, data will not be stored on servers outside Canada.

Reasons

1 through 4, see 2012 Annual PIIDPA report.

5. This survey is the only method of obtaining insights about student engagement and success that can be benchmarked against other institutions in Canada including participants from Nova Scotia.

6. Transfer scholarship funds to Saint Mary's University in payment of student fees.

7. Access required for updating operating software to newer versions.

8. No information is stored outside Canada. Access to data is occasionally required by our Account Manager for the purposes of troubleshooting problems with the service or for installing data into the system. Any time data is accessed by our Account Manager, it is accessed via a secure SFTP site which is physically hosted in Canada.

Université Sainte-Anne

Description

Université Sainte-Anne's student information management system is maintained by a US company called Blackbaud. Storage of the database is in the US.

Conditions

Use of the data is restricted to Université Sainte-Anne as the user and to Blackbaud as the service provider. Distribution to third parties is not permitted unless under a lawful obligation to do so.

Reasons

Hosting services are not available in Canada by the service provider. Legal counsel was obtained to ensure the Université met the PIIDPA requirements prior to giving consent.

University of Kings College

Description

Access to personal information in the custody or under the control of the University of King's College by its employees may have occurred from time to time remotely from locations outside Canada during 2013. A policy governing such access has been circulated within the university and faculty and staff have been briefed on the policy. Access in accordance with the policy is accepted by the University of King's College as appropriate. University employees may have stored personal information in the custody or under the control of the University of King's College on their smartphones and/or laptop computers when travelling outside Canada where necessary for the performance of their employment duties. Storage is also understood to be generally in accordance with the policy. To the best of our knowledge, no other storage of personal information exclusively in the custody or under the control of the University of King's College occurred during 2013.Access and storage of personal information in the custody or under the control of the University of King's College may also have occurred through the use of employees of webmail accounts (e.g., Gmail, Hotmail, Sympatico, etc.); however, we have been advised with respect to faculty that very little personal information is relayed through email, stored on the G drive or in Cloud applications. Most personal information resides in Blackboard, a service provided by Dalhousie University. Because of the integration of some of the university's information technology services with Dalhousie, the University of King's College makes no representations with respect to any of its information stored on or processed through Dalhousie University servers.

Conditions

See provisions 11 through 14 of King's privacy policy. http://www.ukings.ca/files/u42/Kings-Privacy-Statement-FINAL.pdf

Reasons

Access outside Canada to personal information in the custody or under the control of the University of King's College under the policy is only permitted when necessary for the performance of the employee's duties. Without such access, employees would not be able to meet the requirements of their employment. The policy also notes that: Employees must take reasonable precautions to protect the information. For instance, laptops should be secured against theft when travelling and employees should avoid submitting marks or accessing students' personal information online while outside the country.

School Boards[3]

Annapolis Valley Regional School Board

Description

1. One employee of the Annapolis Valley Regional School Board travelled outside Canada for work purposes and had the ability to access personal information contained in email or stored in the GroupWise email system using a Blackberry mobile device. Permission was granted from the head of AVRSB for the use of this device outside of Canada.

2. The Annapolis Valley Regional School Board operates a Twitter account. Twitter is based in the United States. This account is used for sharing news, videos, photos and other information with a broader audience.

3. The Annapolis Valley Regional School Board uses the AESOP System provided by Frontline Technologies Canada (FTC), which is an automated tool used for tracking, processing and storing information related to employee absences and substitute placements.- See description of access or storage provided in the 2012 annual PIIDPA report.

Conditions

1. Remote access to staff email accounts through GroupWise is protected by username/password authentication and is delivered through encryption. Staff mobile devices are also secured with a password.

2. AVRSB uses Twitter to share information and interact online with the public and organizations in social spaces. AVRSB collects no IP addresses or personal information through these services. AVRSB re-tweets other government accounts and information from partners (RCMP, municipalities, health authorities, etc.). Photos and videos that are posted to all social media platforms have written consent from the people in them where required.

3. See description of access or storage provided in the 2012 annual PIIDPA report.

[3] Atlantic Provinces Special Education Authority and Tri-County Regional School Board had no access or storage outside of Canada.

Reasons

1. Staff are expected to monitor email and voicemail for business continuity, and to maintain contact with AVRSB and stakeholders. A Blackberry mobile device was necessary for the staff member to make calls and access email while abroad for work purposes.

2. Social media platforms are used to engage the community, to increase public awareness, and to promote the dissemination of timely, accurate information.

3. See description of access or storage provided in the 2012 annual PIIDPA report.

Cape Breton-Victoria Regional School Board

Description

1. The School Board has contracted the services of Frontline Technologies Canada Inc. (FTC) for the scheduling and placement of substitute teachers, and varying non-teaching classifications in schools, in response to filling casual teacher and non-teaching absences.

The Aesop System provided by FTC is an automated tool used for tracking, processing, and storing information related to teacher absences. Frontline Technologies Canada Inc. utilizes an application service providers (ASP) model for provision of the system to the School Board. The software and data reside in Toronto, Canada and the company is paid a yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. The system is supported and maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA. There are two types of support, technical and end user. Technical support is required to ensure the system is operating as expected and available to the user community, and includes such things as performance management, data backup and recovery, and software upgrades. End user support is needed to assist the School Board with specific system problems being experienced, answer questions regarding software functionality, and provide training information and materials related to new system features. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.

Frontline Placement Technologies were chosen as the successful bidder in response to a Request for Proposal (RFP) that was awarded by the Department of Education (DOE) in October 2007.

Effective 2011/2012 school year this AESOP system was expanded in the Cape Breton-Victoria Regional School Board to include the teacher assistant classification.

Effective 2012/2013 school year this AESOP system was expanded in the Cape Breton-Victoria Regional School Board to also include the cleaners and Lunch/Bus/Ground supervisors.

Effective 2013/2014 school year this AESOP system was expanded in the Cape Breton-Victoria Regional School Board to also include Library Technicians and School Clerical.

2. Approximately five staff members travelled outside Canada and may have, or had the ability to, access personnel information via remote email, blackberry and/or personal computer.

Conditions

1. The Department of Education and seven school boards have signed a five year contract with FTC that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by DOE and the School Board in writing.

The following conditions exist to ensure Nova Scotia's data is protected.

- Frontline has read and agreed to the provisions of the Personal Information International Disclosure Protection Act (PIIDPA) legislation. The contract also has extensive provisions for protection of personnel information, including the requirement for FTC to notify DOE if they receive a foreign order or request to disclose personal information (i.e. an order pursuant to the Patriot Act or similar legislation).

- Frontline Technologies Canada Inc. has contracted data centre services with SunGard Availability Services (SunGard) for housing Nova Scotia's data and the Aesop system infrastructure at their Toronto, Canada location. The School Board data is housed at the SunGard data centre and system support services are provided by FPT located in Philadelphia, USA. Data access by FPT is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and support.

- The following conditions apply when FPT accesses the School Board data i) the accesses must be logged and reported to DOE monthly ii) access is only for the period of time required to address the issue/problem, and iii) access is only carried out from within Canada or from the supplier's secure private network in Philadelphia.

- The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The audits are quite detailed and provide clients with an added level of confidence that SunGard are doing the rights things to ensure continuance of service and protection of information. The audits encompass all areas of the organization including, administration and organization, facilities, logical access, network security, computer operations, backup and recovery processes, and change management processes. SunGard has provided the DOE with a copy of the most recent SAS70 Audit. In addition, the facility is ISO 9001:2000 certified by Lloyd's Registry Quality Assurance.

- All equipment used for the Nova Scotia Aesop implementation is owned by FTC. The equipment is stored at SunGard in individual locked wire cages, and access is restricted to FTC personnel. In addition, SunGard is compliant with industry standards and best practices for data centres; including, privacy of data, separate network segments, remote control cameras, raised flooring, fire detection and suppression systems, cooling, water sensors, electronic monitoring, and uninterruptible power supply systems.

- Employees of FPT have signed confidentiality agreements with the company.

- Only personnel authorized by the School Board will be provided access to the School Board's electronic information.

- The data contained in the system is limited to that required to ensure successful operation. It includes: employee name, professional number, home address, phone number, email address, skill profile including qualifications, work schedule availability, sick leave entitlements, records of absenteeism, teaching assignments completed, and hours worked.

- All personnel information is housed on-site with existing infrastructure. All blackberries, iPhones and personal computers are password protected.

- The DOE on behalf of the school boards issued an RFP for a software solution that would automate the process of filling teacher absences. The school boards evaluated three proposals and selected the Aesop product because of its' superior software functionality and FPT's significant experience in successfully supporting a large user base in other jurisdictions. There was also some experience using this software at one of the school boards, it was found to be a very good product and the vendor support services were excellent. In addition, FTC committed to housing Nova Scotia's data and the Aesop System in Canada to satisfy the DOE concerns with information security and privacy legislation. The DOE and school boards negotiated and signed a contract with FTC in May of 2008. The system began implementation throughout Nova Scotia in September 2008.

- In summary, this solution was chosen because the software is superior to other products on the market and meets the needs of the School Board. The vendor was able to satisfy the DOE concerns regarding protection of information by agreeing to contractual requirements related to Nova Scotia privacy legislation, as well as housing the data and system in Canada. SunGard is a highly reputable and capable organization and were very cooperative in allowing the DOE to conduct and on-site audit of their facility and processes. FTC have signed off on all security and information privacy clauses in the contract, understand and agree to comply with the province's PIIDPA legislation, do not store any data in the US, and use secure methods for all data transmissions. Also all data accesses by employees of the parent company (Frontline Placement Technologies) are restricted to specific purposes and logged and reported to DOE monthly.

2. Functionality of the operations of the board are deemed necessary for management and operations. The staff members at issue occupy management positions and must be available by e-mail.

Reasons

1. **Teacher Professional Development application** – The option of payment by credit card payments as a convenience for teachers, and to provide efficient and effective online services.

2. **Travel with electronic devices** – Staff are sometimes expected to monitor their emails and voicemail for business continuity purposes, and maintain contact with operations. BlackBerry's, iphones were necessary to make calls, access email and internet sites. Laptops are needed for preparing document, and accessing email and internet sites. Permission to take these devises outside the required and to obtain internet packages is required through our School Services division.

Note: We also have our Facebook and Twitter accounts however no personal information is stored and they follow under our Network Access policy. http://lrt.ednet.ns.ca/pdf/naup_2011.pdf

Chignecto-Central Regional School Board

Description

1. A number of Chignecto-Central Regional School Board staff traveled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in the GroupWise email system, using devices including cell phones, iPads, BlackBerrys and laptops.

2. The Chignecto-Central Regional School Board operates a Twitter account. Twitter is based in the United States. This account is used for sharing government news releases, videos, photos and other information to a broader audience.

Conditions

1. Remote access to staff email accounts through GroupWise is protected by username/password authentication and is delivered through a combination of VPN and encryption.

2. The Chignecto-Central Regional School Board uses Twitter to share information and interact online with the public and organizations in social spaces. The Chignecto-Central Regional School Board collects no IP addresses or personal information through these services. The Chignecto-Central Regional School Board re-tweets other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.) Photos and videos that are posted to all social media platforms have written consent from the people in them where required.

Reasons

1. Staff are expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. BlackBerrys were necessary to make calls, access email and internet sites, and make telephone calls. Laptops and iPads are needed for preparing documents and accessing email and internet sites.

2. Social media platforms are used to engage the community, increase public awareness and to promote the dissemination of accurate timely information.

Halifax Regional School Board

Description

1. Ten (10) staff members travelled outside of Canada, who would have had access to personal information via their smartphone, laptop computers or IPads.

2. Twitter is a global communication network that is widely used by people from all over the world. Twitter is instantaneous and immediate. It allows its users to capture anything important that is occurring and share it with the community of followers instantaneously. (Description taken from http://www.educatorstechnology.com)

Conditions

1. Relevant Halifax Regional School Board policies would apply to Blackberry, IPhone, IPad and computer usage outside of Canada. Each smartphone, IPad and computer is password protected.

2. Personal information about students and teachers will be accessed and stored outside Canada as twitter is located outside Canada. There is no acceptable equivalent located within Canada to Twitter. Such access and storage is authorized through determination of "necessity" under S.5(2) of PIIDPA. Such decisions around access and storage will be reported in the report to the Minister of Justice, pursuant to S. 3 of PIIPDA.

Twitter's privacy policy states that their services are not directed to persons under 13. Twitter does not knowingly collect personal information from children under 13. If twitter becomes aware that a child under 13 has provided personal information, twitter will take steps to remove such information and terminate the child's account.

Only the minimum personal information will be provided about students and teachers at the point of setting up new accounts. On the registration form to set up new accounts for teachers and students, it is recommended that the birth dates entered for all students and teachers will be fictitious, and that the field indicating gender should be left blank.

Reasons

1. The staff members involved occupy positions where they must be available by e-mail for decision-making and information and safety purposes.

2. Twitter is used by the Halifax Regional School Board, the Superintendent and various schools to communicate with students, parents and the greater community. This ties directly with the Halifax

Regional School Board's strategic plan goal 1: To improve student achievement and personal success and goals 4: To build engagement, support and confidence in the Halifax Regional School Board.

"Kids and Learning First" identified the need to engage and motivate students. Twitter will enhance the overall education experience.

South Shore Regional School Board

Description

1. Travel with electronic devices: A number of South Shore Regional School Board staff traveled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in the Zimbra email system, using devices including cell phones, iPads, and laptops. Staff seek permission from the head of the public body before taking devices and personal information across the Canadian border. We had 16 instances where these devices were taken outside of Canada.

2. Use of social media: The SSRSB operates a Twitter account. Twitter is based in the United States. This account is used for sharing government news releases, videos, photos and other information to a broader audience.

3. Kahn Academy: The Mathematics Engagement Pilot Project is a project designed to integrate use of the Khan Academy and other digital resources in one to one environments in select schools. Khan Academy resources and interactive lessons are available on a variety of subjects, including mathematics, science, finance, history, and the humanities. Additional apps and resources may be identified as having educational value and may be downloaded or accessed to the devices provided as part of this pilot project. The pilot project will be evaluated to measure its impact on achievement, attendance and engagement and identify any successes. Personal information about students and teachers will be accessed and stored outside Canada as the Khan Academy is located outside Canada.

4. Aesop: The South Shore Regional School Board utilizes the Aesop System provided by Frontline Technologies Canada (FTC), which is an automated tool used for tracking, processing and storing information related to employees absences. The software and data reside in Toronto, Ontario. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. The system is supported and maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.

Conditions

1. Travel with electronic devices: Remote access to staff email accounts through Zimbra is protected by username/password authentication and is delivered through a combination of VPN and encryption.

2. Social media: The SSRSB uses Twitter to share information and interact online with the public

and organizations in social spaces. The SSRSB collects no IP addresses or personal information through these services. The SSRSB retweets other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.) Photos and videos that are posted to all social media platforms have written consent from the people in them where required.

3. Khan Academy: It is recommended that teachers set up Khan Academy student accounts so that all birthdates MUST be from the year 2003. This results in child accounts not turning to full accounts that allow comments and conversations (this activity happens at the age of 13 years). It is recommended that the minimum personal information is provided about students and teachers at the point of setting up new accounts. For example, it is recommended that the birth dates entered for all students and teachers were fictitious, and the field indicating gender was left blank. It is recommended that usernames be the student's or teacher's three initials plus 5-6 numbers, to reduce the ability to easily identify an individual, their gender, or ethnicity. Parents/guardians received information about the project, including any risks associated with participation or using the devices. Curriculum on digital citizenship was delivered to students to promote responsible use of devices, including information on good privacy practices and protecting your own personal information on the Internet. It is recommended that teachers delete all Khan Academy student accounts at the end of the pilot, in June, 2014.

4. Aesop: The Department of Education and Early Childhood Development and the South Shore Regional School Board have signed a further five year contract with Frontline Technology that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by the Department of Education and Early Childhood Education and the School Board in writing. Frontline has read and agreed to the provisions of the Personal Information International Disclosure Protection Act. The contract also has extensive provisions for protection of personal information, including the requirement for Frontline to notify the Department of Education and Early Childhood Education if they receive a foreign order or request to disclose personal information. Data access by Frontline is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and support. Accesses are logged and reported to Department of Education and Early Childhood Education monthly. Access is only for the period of time required to address the issue/problem, and access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The facility is OSO 9001:2000 certified by Lloyd's Registry Quality Assurance. Employees of Frontline have signed confidentiality agreements with the company. Only personnel authorized by the South Shore Regional School Board are provided access to the School Board's electronic information. The data contained in the system is limited to that required to ensure successful operation.

Reasons

1. Travel with electronic devices: Staff is expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. Cell phones were necessary to make calls, access email and Internet sites, and make telephone calls. Laptops and iPads are needed for preparing documents, and accessing email and Internet sites.

1. Social media: Social media platforms are used to engage the community, increase public awareness, and to promote the dissemination of accurate, timely information.

2. Khan academy:It is essential that the education system engages and motivates students, protects rural education, provides information and resources teachers need, links learning to the workplace, and strengthens skills that help students. The Khan Academy is an opportunity to infuse classrooms with technology-based learning that will enhance the overall education experience, particularly in the area of mathematics. There is no acceptable equivalent located within Canada to the Khan Academy and other digital resources that will be accessed by students and teachers in the pilot project. Such access and storage is authorized through determination of 'necessity' under S. 5(2) of PIIDPA.

3. Aesop:PT's Aesop system is functionally superior to other systems on the market and it represents better value. FPT's support model is preferred. A pilot project with Aesop was successful. For these reasons, the decision to select FPT as the vendor was to meet the 'necessary requirements of the public body's operation.

Strait Regional School Board

Description

1. Forty-four (44) Regional School Board staff traveled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in the Webmail email system, using devices including cell phones, iPads, BlackBerrys and laptops. Staff seek permission from the head of the public body before taking devices and personal information across the Canadian border.

2. The Strait Regional School Board utilizes the Aesop System provided by Frontline Technologies Canada (FTC) which is an automated tool used for tracking, processing and storing information related to employees (some bus drivers, teacher assistants, secretaries, library technicians, teachers, administrative support staff, regional office, non-union support and all teachers, substitutes and casuals for all previously mentioned classifications) absences. FTC utilizes an application service provider (ASP) model for provision of the system. The software and data reside in Toronto, Canada and the company is paid a yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. The system is supported and maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA. There are two types of support, technical and end user. Technical support is required to ensure the system is operating as expected and available to the user community, and includes such things as performance management, data backup and recovery and software upgrades. End user support is needed to assist the School Board with specific system problems being experienced, answer questions regarding software functionality, and provide training information and materials related to new system features. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.

3. The Board currently holds online subscriptions for Learning A to Z. These are on line subscriptions to education media. The teacher's name and school are provided to both online education media providers. This contract is a yearly subscription.

4. The Strait Regional School Board operates a Twitter account. Twitter is based in the United States. This account is used for sharing news releases, videos, and other information to a broader audience.

Conditions

1. Remote access to staff Webmail through email accounts is protected by username/password authentication and is delivered through a combination of VPN and encryption.

2. The Department of Education and Early Childhood Development and the Strait Regional School Board have signed a further five year contract with Frontline Technology that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by the Department of Education and Early Childhood Education and the School Board in writing. Frontline has read and agreed to the provisions of the Personal Information International Disclosure Act. The contract also has extensive provisions for protection of personal information, including the requirement for Frontline to notify the Department of Education and Early Childhood Education if they receive a foreign order or request to disclose personal information. Data access by Frontline is restricted and only permitted on an as required basis in response to requests from the School Board or for system maintenance and support. Accesses are logged and reported to the Department of Education and Early Childhood Education monthly. Access is only for the period of time required to address the issue/problem, and access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. The SunGard facility is audited regularly by independent firms to ensure verification of process and discipline. The facility is OSO 9001:2000 certified by Lloyd's Registry Quality Assurance. Employees have signed confidentiality agreements with the company. Only personnel authorized by the Strait Regional School Board are provided access to the School Board's electronic information. The data contained in the system is limited to that required to ensure successful operation.

3. Service provider has a confidentiality agreement in place.

4. The Strait Regional School Board uses Twitter to share information and interact online with the public and organizations in social spaces. The Strait Regional School Board collects no IP addresses or personal information through these services. The Strait Regional School Board retweets other government accounts (including other School Boards), School accounts, RCMP, Department of Education and Early Childhood Development, Nourish Nova Scotia, etc. Photos and videos that are posted to all social media platforms have written consent.

Reasons

1. Staff is expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. BlackBerrys were necessary to make calls, access email and Internet sites, and make telephone calls. Laptops and iPads are needed for preparing documents, and accessing email and Internet sites.

2. FPT's Aesop system is functionally superior to other systems on the market and it represents better value. FPT's support model is preferred. A pilot project with AESOP was successful. For these reasons, the decision to select FPT as the vendor was to meet the 'necessary requirements of the public body's operation'.

3. These resources are not available in Canada. Only minimal personal information is shared which is voluntary.

4. Social media platforms are used to engage the community, increase public awareness, and to promote the dissemination of accurate, timely information.

Municipalities[4]

Halifax Regional Municipality

Description

1. Versaterm (Police RMS, CAD 911), with a Canadian headquarters in Ottawa, ON were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes (see 2012 Annual PIIDPA Report).

2. Between January 1st and December 31st, 2013, thirty-two (32) HRM staff and three (3) HRP staff travelled outside of Canada and had the ability to access personal information via one or more of the following means: Cell Phone, Blackberry, Laptop, Memory Stick, VPN (see 2012 Annual PIIDPA Report).

3. Open Text (Document Management), with a Canadian headquarters in Waterloo, ON were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes (see 2012 Annual PIIDPA Report).

4. Hastus ERP (Metro Transit), with a Canadian headquarters in Montreal, QC were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes (see 2012 Annual PIIDPA Report).

5. RIVA (PSAB Compliance Financial - Assets), with a Canadian headquarters in Toronto, ON were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes (see 2012 Annual PIIDPA Report).

6. SAP (Finance, HR and Crystal Reports), with a Canadian headquarters in Toronto, ON were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes (see 2012 Annual PIIDPA Report).

7. ESRI (GIS), with a Canadian headquarters in Toronto, ON were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes (see 2012

[4] Cape Breton Regional Municipality, Cumberland Joint Services Management Authority, Pictou County Shared Services Authority, Halifax Public Libraries, South Shore Public Libraries, Town of Annapolis Royal Public Works, Municipalities of the Counties of Annapolis, Cumberland, Kings, Victoria, Municipalities of the Districts of Argyle, Barrington, Clare, Guysborough, Lunenburg, Shelburne, West Hants, Towns of Antigonish, Berwick, Clark's Harbour, Digby, Hantsport, Inverness, Kentville, Lunenburg, Mahone Bay, Mulgrave, New Glasgow, Parrsboro, Port Hawkesbury, Shelburne, Stellarton, Stewiacke, Trenton, Truro, Westville, Windsor, Yarmouth, Region of Queens Municipality had no access or storage outside of Canada to report. The Town of Oxford did not provide a completed PIIDPA Form 1.

Annual PIIDPA Report).

8. IVOS (Claims/Risk Management) with a Canadian headquarters in Toronto, ON were provided access on an approved need basis to the applicable production systems for support and maintenance purposes (see 2012 Annual PIIDPA Report).

9. Messaging Architects (Email Archive), with a Canadian headquarters in Montreal, QC were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

10. Niche (Digital Mug Shot) with a Canadian headquarters in Winnipeg, MB were provided access on an approved need basis to the applicable production systems for support and maintenance purposes (see 2012 Annual PIIDPA Report).

11. Trapeze (Transit) with a Canadian headquarters in Mississauga, ON were provided access on an approved need basis to the applicable production systems for support and maintenance purposes.

12. WinTik (Scale Management System, Solid Waste) with a Canadian headquarters in Kanata, ON were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

13. Active Networks (Recreation Class Registration) with a headquarters in San Diego, CA were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

14. Fleet Focus (Fleet Management, TPW) with a headquarters in Calgary, AB were provided access on an approved, need basis to the

15. EMC (Storage Area Network, VMWare) with a headquarters in Toronto, ON were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

16. City Watch (Public Safety Notification) with a headquarters in Bloomington, MN were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

17. Safran Morpho (Digital Mug System) with a headquarters in Montreal, QC were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

18. Microsoft (Email, Office, Sharepoint, File Shares) with a headquarters in Mississauga, ON were

provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

19. Research in Motion (Blackberry) with a headquarters in Waterloo, ON were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

20. Service Providers - Service Now, IT Service Relationship Management with a headquarters in Santa Clara, CA - HRM's data is hosted in Canada.

21. Service Providers Blackbaud, Fund Raising Management for Halifax Public Library, with a headquarters in Vancouver, BC - HRM's data is hosted in Canada.

22. Service Providers Kenexa - Brassring, HR Applicant Tracking System, with a headquarters in Wayne, PA.

23. Service Providers Scotiabank and Merchant Card Services partner, Chase Paymentech, with a Canadian headquarters in Toronto, ON provide banking services.

Conditions

1 through 10, see conditions provided in the 2012 annual PIIDPA report.

11 through 19, Vendor access is controlled and monitored by IT Support staff.

20 through 22, Service providers are bound by duly executed agreements that detail their obligations for the protection, use and disclosure of personal information.

23. See description provided in the 2012 annual PIIDPA report.

Reasons

1. Vendor access is necessary for the system to continue to function properly.

2. The HRM and HRP staff, who travelled outside of Canada with their communication device(s) were expected to maintain a means of communication with their respective staff/Business Unit in order to meet operational responsibilities/requirements.

3 through 18. Vendor access is necessary for the system to continue to function properly.

19 through 23. Service providers were secured through the RFP process and achieved the highest overall proposal evaluation scoring and provided the best financial value for the municipality.

Halifax Water Commission

Description

1. Between January 1, and December 31, 2013, thirty-seven (37) Halifax Water staff were permitted to transport personal information devices, such as laptop computers, cell phones, and electronic data storage devices outside Canada seventy-five (75) times. The following vendor: Tokay Navigator Software, Framingham, Massachusetts, provides initial customer data conversion and upload, periodic software maintenance and upgrades, and customer technical support.

Conditions

1. See description of access or storage provided in the 2012 annual PIIDPA report.

Reasons

1. See description of access or storage provided in the 2012 annual PIIDPA report.

Municipality of the County of Colchester

Description

Ten (10) staff members traveled outside Canada during calendar year 2013. It is known that five staff accessed personal email or stored information and email either through Outlook, via a laptop or Blackberry. The employees received permission from Senior Management.

Conditions

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.

Reasons

When staff are traveling 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 East Hants

Description

Thirteen (13) employees left the country, with access to personal information.

Conditions

All municipal devices, (cell phones, laptops) and accounts are password protected.

Reasons

When staff are travelling for business or personal reasons, they may be expected to monitor their business email in order to fulfill their job responsibilities.

Municipality of the County of Pictou

Description

When staff travel outside the country for business, training or pleasure, they may be required to monitor their email and voicemail to deal with urgent ongoing matters. Therefore, it is necessary for them to work. Several employees within the Municipality of Pictou County travelled outside of the country with their Municipally owned electronic devices. During this time, employees had access to the email system from their mobile devices.

Conditions

All devices were password protected and the laptop information was encrypted.

Reasons

When staff travel outside the country for business, training or pleasure, they may be required to monitor their email and voicemail to deal with urgent ongoing matters. Therefore, it is necessary for them to work.

Municipality of the County of Richmond

Description

Five employees travelled outside of Canada - laptop, blackberries and iPads were used.

Conditions

All devices are password protected.

Reasons

Travelling for work purposes access to email required to stay connected with office.

Municipality of the District of Chester

Description

Five (5) employees travelled outside of Canada, there was a need to provide remote support to the organization, stay in touch with the CAO on ongoing planning and development matters, and stay in touch regarding emergency measures issues while away.

Conditions

N/A

Reasons

The nature of the access was required to fulfill business obligations of the Municipality of the District of Chester.

Municipality of the District of Yarmouth

Description

Three employees travelled outside Canada and had the ability to access personal information via one or more of the following means: cell phone Blackerry and laptop.

Conditions

All devices were password protected and the laptop information was encrypted. Access to our network was through our VPN.

Reasons

When staff travel outside the country for business, training or pleasure, they may be required to monitor their email and voice mail to deal with urgent ongoing matters. Therefore, it is necessary for them to work remotely, where possible, in order to fulfill their responsibilities.

Property Valuation Services Corporation

Description

PVSC uses "Time Out" – a vacation tracking and scheduling software provided by CWS Software based in New Jersey, NY, USA. This software is used by PVSC employees for internal use only.

Conditions

PVSC employees can access only their own personal records in "Time Out" with the exception of managers who access the information relevant to the staff they supervise. The only information stored that meets the criteria of "personal" under PIIDPA is the employee names. The contract with CWS contains appropriate confidentiality clauses and provisions for destruction of information upon request.

Reasons

The software is required for appropriate time management and tracking of PVSC employees.

Town of Amherst

Description

Four (4) Town of Amherst staff travelled outside Canada during the calendar year 2013 and had the ability to access personal information via BlackBerry, iPhone, iPad and laptop computer. Prior approval to travel outside Canada with mobile devices was obtained from the CAO. Human Resource overtime, vacation and sick time information is stored within EZ Labour, a product offered by ADP.

Conditions

Email access requires authentication through secure time-limited login/password. VPN is used to access electronic data remotely. In terms of the human resource information in EZ Labour, authentication through secure, time-limited login/password is required.

Reasons

Senior staff travelled for business or personal reasons; they were expected to monitor their business email in order to fulfill their job responsibilities during such absences. They were required to submit an application for CAO's approval to take any mobile devices outside Canada. The Town of Amherst only recently became aware that HR data in EZ Labour was stored outside Canada. We are actively investigating alternatives.

Town of Annapolis Royal

Description

1. One Municipal Elected Official travelled outside Canada and had the ability to access personal information via a Blackberry device. Appropriate permissions were granted.

2. Since approximately 2003, the Town website has been facilitated by a private firm and the website has been hosted in a most reputable web host in Utah and Texas. We are considering moving the Town website to a Canadian-based host.

3. Since approximately 2003, the Town email has been facilitated by Google Mail service. We are considering moving Town email away from Google Mail to be hosted by a Canadian host.

Conditions

1. Official has been advised that the use of communication device that can gain access to personal information, to limit email use during the time out of the country. Prior to travelling, they were required to report their intentions to the PIIDPA Administrator to ensure secure login/passwords and encryption protocols were and are, in place.

2. N/A

3. N/A

Reasons

1. Municipal Official was expected to monitor email in order to fulfill responsibilities/requirements.

2. The decision was made in 2003. The location of the service provider is now identified and the website is being considered to be moved to a host in Canada.

3. The decision was made in 2003. We are considering moving Town email away from Google Mail to be hosted by a Canadian host.

Town of Bridgetown

Description

1. All critical data is housed on site at the Town of Bridgetown offices. The website data, all public data accessible from the internet is housed on a server outside Canada.

2. Website is hosted by Westcliffe Marketing (local owner, Hampton, Nova Scotia, Canada (Nova Scotia, Canada). No personal information is stored or disseminated via the website.

Conditions

No data is accessed by a third party not located in Canada. The IT consultant on contract uses the VPN to access data on site but this is all within Nova Scotia.

Reasons

N/A

Town of Bridgewater

Description

Eleven staff/councilors travelled outside of Canada and have the ability to access Town of Bridgewater information via one or more of the following technical means: cell phone, laptop, flash drive or Blackberry. However, a large portion of staff had chosen to leave their devices at home; several chose to "disengage" access to the Town's information all together.

Conditions

The Town of Bridgewater has a Network and Internet Acceptable Use Policy (Policy #61) in place which includes international travel. All devices are to be password protected. The Town also provides a "dummy" laptop for use by staff. The "dummy" laptop does not contain any data and has to be signed on "remotely" with secured login/password.

Reasons

If required, elected officials for the Town of Bridgewater, monitor emails in order to fulfill their responsibilities/requirements.

If required, under specific circumstances, Departmental Directors/Heads may be expected to monitor emails and carry out specific duties in order to fulfill their job responsibilities if travelling was necessary at that time.

Town of Middleton

Description

1. All critical data is housed on-site at the Town of Middleton offices. The website data, all public data accessible from the internet is housed on a server outside Canada. The website is hosted by Westcliffe Marketing (local owner, Hampton, Nova Scotia). No personal information is stored or disseminated via the website.

2. On occasion, municipal councilors will travel outside of Canada and take with them a tablet device that has access to the municipal email system and internal document management system. All these files are physically stored at the Town of Middleton offices. Tablet devices are accessing data through a SSL layer and have passcodes to limit unauthorized access and remote wipe capabilities should the devices be lost or stolen.

3. The Town of Middleton does have a Facebook account for the purpose of disseminating information to the public via the social media stream.

Conditions

No data is accessed by a third party not located in Canada. The IT consultant on contract uses the VPN to access data on site, but this is all within Nova Scotia.

Reasons

N/A

Town of New Glasgow

Description

Several employees within the Town of New Glasgow travelled outside of the Country with their Town of New Glasgow owned electronic devices which had been requested and approved by their supervisor and Chief Administrative Officer based on their job role within the Municipality. During this time, employees had access to the Town's email system from their Blackberry devices, iPhones, iPads and other smartphone devices.

Conditions

Blackberry devices are encrypted and also have a device password provisioned and are under the control of the Town's internal BlackBerry Enterprise Server. Remote access to webmail is encrypted with SSL and protected with usernames and passwords which are changed on a regular basis. Both iPhones & iPads and other Android devices are provisioned and controlled by the Town's internal Mobile Device Management Server (MDM).

Reasons

Employees or Elected Officials from the Town of New Glasgow may request to travel out of the Country with their Town provided electronic devices. A process has been put in place where the requesting user must fill out a form and submit to their department head/supervisor to request permission to travel outside of the Country with a Town provided electronic device. Final decision remains with the Chief Administrative Officer. The Chief Administrative Officer will review the request from the employee or elected official and decide based on their role with in the Municipality if it is necessary for the user to travel with the device; such as senior staff or members of Council within the Municipality and senior officers within the Town's Regional Police Agency.

Town of Wolfville

Description

All critical data is housed on site at the Wolfville offices. The Website data, all public data accessible from the internet is housed on a server in Canada. Website is hosted by Colibri-Software (www.colibri-software.com). No personal information is stored or disseminated via the website.

Conditions

No data is accessed by a third party not located in Canada. The IT consultant on contract uses the VPN to access data on site, but this is all within Nova Scotia.

Reasons

The Town of Wolfville has made significant investment in mobile technology (iPad and iPhone), the convenience and flawless operation of the Drop-box service justifies the transfer of transient data to this service for temporary access on the mobile devices.