Personal Information International Disclosure Protection Act

2014 Annual Report

Department of Justice

July 2015

NOVA SCOTIA

Message from the Minister of Justice

I am pleased to provide the ninth 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 1st, 2014, to December 31st, 2014, to the Minister of Justice. This report is based on the *PIIDPA* reports received by the Policy and Information Management Division of the Nova Scotia Department of Justice.

This report contains a summary of the 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.

Original signed by

The Honourable Lena Metlege Diab, ECNS

Minister of Justice and Attorney General

Table of Contents

Methodology

Section 5(3) of the *Personal Information International Disclosure Protection Act (PIIDPA)* has a mandatory requirement that all access and storage of personal information outside of Canada must be reported to the Minister of Justice within ninety days after the end of the calendar year that the access or storage occurred.

On January 23rd, 2015 a request was sent to public bodies[1] in Nova Scotia to complete and return a *PIIDPA* Form 1 for the 2014 reporting year by March 31st, 2015. Public bodies were given the option of submitting their information through a web-based survey or by completing a Form 1 and submitting it directly to the Department of Justice. Subsequently, two notices were sent as a reminder of the requirement to report.

The 2014 Annual *PIIDPA* report is a reproduction of the information that was provided to the Minister of Justice by reporting public bodies and is not a validation of content or compliance. Non-respondent entities are recorded in the report as "did not provide a completed *PIIDPA* Form 1".

Due to changes in the organizational structure of public bodies, comparisons over time should not be made.

---

[1] "Public body" as defined by the *Freedom of Information and Protection of Privacy Act* means (i) a Government department or a board, commission, foundation, agency, tribunal, association or other body of persons, whether incorporated or unincorporated, all the members of which or all the members of the board of management or board of directors of which (A) are appointed by order of the Governor in Council, or (B) if not so appointed, in the discharge of their duties are public officers or servants of the Crown, and includes, for greater certainty, each body referred to in the Schedule to this Act but does not include the Office of the Legislative Counsel, (ii) the Public Archives of Nova Scotia, (iii) a body designated as a public body pursuant to clause (f) of subsection (1) of Section 49, or (iv) a local public body. "Public body" also includes municipalities as defined by Part XX of the *Municipal Government Act* where "municipality" means a regional municipality, town, county or district municipality, village, service commission or municipal body.

Key to Submitted PIIDPA Reports

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

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

C: Statement of how the decisions to allow 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

Foreign Access and Storage by Government Departments[2]

Agriculture

Description

1. Remote Access via electronic devices such as BlackBerrys, laptops, and tablets. There were five (5) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email.

Staff	Date	Country
Staff #1	April 2014	USA
Staff #2	October 2014	USA
Staff #1	November 2014	USA
Staff #3	November 2014	USA
Staff #4	November 2014	USA
5 instances total		

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 Information, Communications and Technology Branch (ICTS) recognized the limited options available for a new V-LIMS system, they were cautious about the security of the system on their server. ICTS' 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 an electronic device 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 government issued electronic devices 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.

---

[2]The Department of Seniors and Office of Aboriginal Affairs did not have 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. ICTS' 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.

Communications Nova Scotia

Description

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. 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. Seven employees of CNS travelled to the United States with BlackBerrys. Four of the employees also had iPads and one had a laptop.

Conditions

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 only by Communications Nova Scotia employees.

Reasons

Communications Nova Scotia is accountable in our business plan to report on the effectiveness of major Internet (and other) campaigns. Use of Google Analytics enabled us to collect and report on accurate statistics about how many visitors came to our websites, from where, and approximately how long they stayed. This information allows us to refine our marketing and advertising strategies ensuring that we provide best value to the government. 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 used to make calls and use email. The iPads and laptop were used to email, post messages on Facebook, access Twitter and for writing material.

Communities, Culture and Heritage[3]

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 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 Nova Scotia Archives website enables Internet visitors to access the photostream without a Flickr account. Visitors also able to comment on content via phone or email 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. Continued use of Twitter and Facebook accounts (see previous PIIDPA Report).

5. Ebook access (eLending) has quickly become a critical service that libraries provide to clients. A technical change made by our existing service provider (OverDrive) has led to the

[3] Report includes Acadian Affairs, African Nova Scotian Affairs and Nova Scotia Archives and Records Management.

storage of the personal information of libraries users on servers outside of Canada (previously, it authenticated against our locally-housed database). The OverDrive platform, used by libraries to circulate digital materials (primarily ebooks and audiobooks) to library users, has changed from using Adobe IDs to enforce the Digital Rights Management (DRM) applied to individual titles, to an account-based model. New users are required, and most existing users, will need to create OverDrive accounts to improve user experience and eliminate usage barriers created by Adobe IDs.

New OverDrive accounts contain personal information about identifiable individuals (library clients in Nova Scotia), including name, email address and/or Facebook information. This personal information is voluntarily provided when a client registers for the OverDrive service. OverDrive collects certain information about client interactions with them and information related to clients and their use of the Service, including but not limited to, Personal Information, online activity, digital content selections, reviews and ratings, as well as Internet Protocol addresses, device types, unique device data, such as device identifiers, and operating systems.

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. The service provider (Unisys Canada Inc./ACOL contract) is PCI-compliant.

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 enables SirsiDynix to access the server for specific upgrade activities at predetermined time periods, at the end of which SirsiDynix staff are logged out by NSPL staff.

   NSPL staff monitor and audit to ensure the access is reasonable and appropriate.

   SirsiDynix has no operational requirements to access personal information about clients.

   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 has* been completed on this project.

Any issues that were discovered were quickly addressed by NSPL and the appropriate regional library board.

4. N/A

5. Efforts were made to ensure that Privacy information was readily accessible to service users. The OverDrive "privacy policy" and "terms and conditions" clearly state what personal information is collected, the information that can be associated with users and the ability for users to "opt out" of data collection metrics. There is also the ability for individuals to clear their borrowing history and delete associated cookies from devices.

   OverDrive complies with the U.S. – EU Safe Harbor Framework and the U.S. – Swiss Safe Harbor Framework regarding the collection, use, and retention of Personal Information.

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

5. With the increased availability of technology and mobile devices, libraries are expected to provide access to digital media that is accessible to all of their users. At the time that OverDrive was purchased, it was the only viable competitor in the electronic lending market. While competition is starting to grow in the market, there is not currently a viable Canadian alternative for either the platform, or the breadth of service available to library users

through the OverDrive platform. The company serves customers worldwide from its base in the United States.

Community Services[4]

Description

1. A staff member took her phone with her when she went to New York from June 9th to 16th, 2014.

2. Children in Care of the Minister of Community Services may require treatment services that are not available in the Province of Nova Scotia, and on occasion within Canada. During the 2014 calendar year, five children in care were placed in residential treatment facilities in the United States to receive residential treatment services. As part of the referral for placement to a treatment facility, information concerning the child, any medical diagnosis, treatment needs and relevant family information is shared with the placing facility. This information is provided to ensure that the facility will be able to meet the child's clinical needs and for the purpose of developing an appropriate treatment plan for the child. Information provided to the placing facility would include electronic information such as emails with agency social workers in Nova Scotia and paper copies of information identified above.

3. 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.

4. A staff member travelled to England in July 25th to August 8th 2014 with her government issued smart phone. As per policy permission was granted by Deputy Minister prior to departure.

5. Since 2000, Community Services has stored approx. 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 do 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 United States.

6. Two employees travelled outside of Canada with an IPhone.

---

[4] Report includes the Advisory Council on the Status of Women

Conditions

1. N/A

2. Information provided in these situations is to be used solely for the purpose of the determination of placement and the development of treatment plans for children.

3. 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.

4. N/A

5. 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.

6. Devices were password protected.

Reasons

1. The staff member took her phone for business purposes.

2. Information provided to the placing facility is stored in accordance with the Health Insurance Portability and Accountability Act (HIPPA) of 1996. The information is stored in a locked environment on the facility campus for a period of not more than six years, or until the client reaches the age of 22, whichever is the longest. Information is released only with written request by the legal guardian or client, when the client has reached the age of 18 years.

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

4. Permission was granted for the staff member to travel with her smart phone in order to facilitate any departmental emergency contact needs while she was out of the country.

5. 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.

6. Necessary to make calls and access email for business purposes.

Economic and Rural Development and Tourism

Description

1. Staff members were approved to take BlackBerrys out of country on 34 instances in 2014.

2. NSTA uses Curalate to monitor how NSTA images are used in an online platforms such as Instagram, Pinterest, and Facebook. Curalate has a contest management tool which was used by NSTA to gather Instagram images of Nova Scotia for the Doers & Dreamers Guide and on the novascotia.com website. The software collected names and email addresses of those who choose to enter their photos in the contest.

Conditions

1. Remote access to email is protected by username/password authentication and is delivered over a secure server link.

2. Participation in the contest is voluntary. Information collected is limited to firstname, lastname and email address. Potential contestants were informed that their information will be stored in the US. They may contact NSTA to change/delete their data at any time. NSTA obtained an agreement from Curalate that the data would be deleted from the US servers once it was transferred to NSTA.

Reasons

1. Staff members out of the country on government business must be able to access their email and maintain communication with their home office.

2. NSTA used the contest component of Curalate to generate interest, content and new email subscribers. It fed directly into the Tourism strategy and the goal of being a leader in the use of on-line technology to market the province

Education and Early Childhood Development

Description

1. 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. 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. The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the United States for payment authorization and reconciliation. Personal information that is transmitted through or stored outside Canada is at risk of a foreign demand for disclosure.

4. The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the United States for payment authorization and reconciliation. Personal information that is transmitted through or stored outside Canada is at risk of a foreign demand for disclosure.

5. The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the United States for payment authorization and reconciliation. Personal information that is transmitted through or stored outside Canada is at risk of a foreign demand for disclosure.

6. The Alert Solutions software (auto-dialer software) was implemented in all English-language school boards.

7. A number of Department of Education and Early Childhood Development staff travelled 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. Department of Education and Early Childhood Development staff seek permission from the head of the public body before taking devices across the Canadian border.

8. The Department 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. 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. 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. 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. 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.

6. The datacenter is in Toronto, and the US based company supports the system including accessing the data for the sole purpose of responding to operational requests from school boards.

7. 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.

8. 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.

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 students, and provides efficient and effective online services, especially where the students are located around the world.

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

6. The software is integrated with PowerSchool. Utilizing voice, SMS text and email, school administrators can send messages to parents and staff instantly and reliably. Communication

with our audiences is essential, especially for school cancellations, times of emergencies, etc.

7. Staff are expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. Cellular 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.

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

Energy

Description

Twenty-four employees accessed their government email while travelling outside of Canada on business or personal travel. Individuals used their government-issued cellular phone or the remote Outlook access to view their Government email account from a computer (BlackBerry™, laptop, wireless devices, and direct link). Individuals may have also travelled with a government-issued laptop computer. Access of personal information would have been restricted to information in the contacts directory of their device.

Countries visited include: France, Malaysia, Netherlands, the United Kingdom, United States, Norway, China, Korea, Germany and Chile. Staff took 87 personal and business trips outside of the country in 2015 in which they accessed government email while out of the country.

Conditions

Staff use of government-issued BlackBerry devices provides email delivered over an SSL-encrypted link via the secure BlackBerry server. 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

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

One employee travelled for work outside of Canada with a laptop computer.

Conditions

All devices used during travel outside of Canada were password protected.

Reasons

The laptop was necessary to complete work while travelling and to access email for business continuity purposes.

Executive Council

Description

Two employees travelled outside the country on personal leave with their iPad devices; one employee did the same with both iPad and BlackBerry. All obtained the permission of their Deputy Minister under the Out-of-Country Travel Policy.

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.

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. 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.

Finance and Treasury Board

Description

Remote Access via BlackBerry or other electronic devices. There were 4 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.

Fisheries and Aquaculture

Description

1. Remote Access via electronic devices such as BlackBerrys, laptops, and tablets. There were three (3) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email.

Staff	Date	Country
Staff #1	March2014	USA
Staff #2	October2014	USA
Staff #1	November2014	China
3 instances total		

Conditions

1. Permission must be granted in order to take an electronic device 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 government issued electronic devices 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 of Health and Wellness outside of Canada from January 1, 2014 to December 31, 2014.

However, the Reproductive Care program used a new service that resulted in email address' being stored outside of Canada, as reported below.

1. Reproductive Care Program - In 2014 the Nova Scotia Reproductive Care Program (RCP) used the services of a company called iContact to distribute two Program newsletters to health professionals in Nova Scotia and beyond. The iContact company is a cloud based email provider located in Raleigh, North Carolina. Our understanding had been that iContact did not store the email information uploaded each time a newsletter is distributed however, this was a misunderstanding on RCP's part. While email addresses are not stored on the company's general server, they are stored on a section associated with our account to enable the company's 'unsubscribe' feature. RCP discontinued this method of distributing the Program's newsletter once this issue was discovered.

Access: The Department of Health and Wellness continued the following approvals for access to personal information in the custody or control of the Department of Health and Wellness outside of Canada from January 1, 2014 to December 31, 2014.

2. Language Line Services HealthLink 811 - Language Line Services was subcontracted 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.

3. McKesson Corporation, Relay Health HealthLink 811in 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. The work in the information system is monitored by local 811 technical support. Information is accessed only and no information is saved, transferred or replicated by Relay Health staff in the U.S.

4. McKesson Corporation, Secure Health Access Record (SHARE) McKesson developers need to access the provincial Electronic Health Record (SHARE) system from their offices, outside of Canada to deploy software changes and test the upgrade software. 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 on 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 DHAs/IWK/Department of Health and Wellness / HITS-NS staff using the application and audit log data.

6. DHW Employee Access: Between January 1, 2014 to December 31, 2014 nine (9) staff of the Department Health and Wellness were granted approval to travel outside Canada on business with their mobile devices and therefore had the ability to access personal information via email or in documents if saved on their device (e.g., downloading PDFs to read on device)

Conditions

1. Reproductive Care Program - The email addresses of newsletter subscribers were not stored on the iContact general server. They were stored on a section associated with RCP's account to enable the (thought to be) required 'unsubscribe' feature.

2. Language Line Services HealthLink 811Language 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.

3. McKesson Corporation, Relay Health HealthLink 811In rare circumstances, Relay Health may be granted remote access from outside Canada when supporting local IT on a technical issue for resolution at the work station and call center levels.

4. McKesson Corporation, Secure Health Access 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 be stored outside of the country. When required, McKesson's development staff will use a pre-existing secure 'data tunnel' to connect the McKesson test system to complete any required 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 developer's/testers access will be terminated immediately at test completion. 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. 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 email unless encrypted and sent via secure file transfer protocol. This has been communicated through training, and will continue to be reinforced. Therefore, the amount of personal information held or sent by email, and therefore available for access while staff were outside the country, should be limited. All BlackBerry devices and laptops issued by the Department are automatically password protected.

Reasons

1. Reproductive Care Program - The iContact service did not meet the necessary requirements. RCP discontinued this method of distributing the Program's newsletter once this issue was discovered.

2. Language Line Services HealthLink 811McKesson 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.

3. McKesson Corporation, Relay Health HealthLink 811McKesson Canada's partner in the development of the Teletriage application is Relay Health. As a result, Relay Health is the only available provider of third level technical support for the information technology application that enables HealthLink811 operations.

4. McKesson Corporation, Secure Health Access Record (SHARE) The McKesson product used for the provincial SHARE system is proprietary to McKesson so no other vendor can perform the changes. The McKesson code and product development site is located in the United States. 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 is travelling for business reasons (e.g. meetings, conferences) they are expected to monitor their email and voice mail where possible. Therefore it is necessary for them to check email remotely where possible in order to fulfill their responsibilities. As per PIIDPA, any employees that meet this need must submit their request for approval by the Minister of Health and Wellness.

Intergovernmental Affairs

Description

3 Staff Members took BlackBerrys and, on some occasions, laptops out of the country on Business Related Travel a total of 14 times.

Conditions

BlackBerrys were bound to policies as set out by the BlackBerry Enterprise server including passwords and timed lock outs. Laptops were password protected and no data was stored on the laptops themselves, it was only accessed via VPN connections.

Reasons

The decision was made to enable staff to fulfill their functions while abroad. The devices were needed to communicate with home office and receive relevant information.

Internal Services[5]

Description

1. Travel outside Canada - There were 8 instances for which staff were approved to take a BlackBerry or other electronic device while travelling outside of Canada and may have accessed personal information.

2. Operational Accounting - This service was incorporated in the new Internal Services department on April 1, 2014. There has been no changes since the 2013 Finance and Treasury PIIDPA report, as follows:

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

---

[5] The Department of Internal Services (ISD) was created on April 1st, 2014. The *PIIDPA* report for ISD includes the following: Information Communication and Technology Services (former Chief Information Office), Procurement, Payment Transaction Services, Operational Accounting, Payroll Client Relations, SAP Support, Internal Audit, Queens Printer, Information Access and Privacy, Real Property (including land acquisition and disposal), Public Safety and Field Communications, Building Services, Environmental Services, Insurance and Risk Management and Nova Scotia Lands.

3. SAP Service Management - This service was incorporated in the new Internal Services department on April 1, 2014. As with Operational Accounting mentioned above, there has been no changes in personal information access or outside Canada since the 2013 Finance and Treasury PIIDPA report, as follows:

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

4. Risk Management and Security Services - CS STARS LCC has been awarded the contract to supply and support its licensed software (STARS) which will be used by the Risk Management and Security Group for claims management and insurance inventory for the Province of Nova Scotia. Stars was chosen because it met the necessary operational requirements of the Risk Management and Security Group. The data will be stored on the Stars server in Chicago and the system will be executed remotely by IRM on a server located here in Halifax.

5. Expense Management System - 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 Tangoes 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. Travel outside Canada - BlackBerrys or other electronic devices utilized by staff outside the country were protected by passwords, encryption (in some cases) and by all the security means established by the Province. 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.

2. Operational Accounting
   - RBC has entered into a service agreement with the Province of Nova Scotia. The terms set out consider the automated clearing houses (ACHs) required to process electronic vendor payments outside Canada. RBC is required to report to the Minister of Finance all unauthorized access or foreign disclosure of personal information.
   - All Automated Clearing House (ACH) Payments are governed by the National Automated Clearinghouse Association (NACHA) because of the sensitivity of the data on the files.
   - Use of ACH data for purposes other than to complete the transfer of the funds is not endorsed by NACHA and in some cases may be illegal. Each bank in the US must comply to the rules of NACHA

- Vendors opt into receiving electronic payments. They are required to complete an application form, consenting to have payments forwarded to them via our electronic vendor payment (EVP) system.

3. SAP Service Management - 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.

4. Risk Management and Security Services - CS STARS LLC has read, understands, and signed off on its obligations under the Nova Scotia Act. At any time, if required, Provincial Government employees may travel to CS STARS offices in order to inspect the security measures that have been put in place to protect personal information belonging to the Province of Nova Scotia.

5. Expense Management System - 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. ICTS 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 Tangoes offices to inspect the security measures Tangoe has in place.

Reasons

1. Travel outside Canada - Staff attending business events outside Canada may be approved to take assigned BlackBerry or other electronic devices with them to ensure seamless workflow and service continuity.

2. Operational Accounting
   - 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 US requires that information flows through an Automated Clearing House.
   - There is no ACH that stores information in Canada.

3. SAP Service Management - 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.

4. Risk Management and Security Services - After reviewing the Province's business requirement, IT Management recommended implementation of ASP Stars as it fit the operational requirements of the Risk Management and Security Group and there wasn't a cost effective Canadian solution available.

   The STARS system has been in operational use by Government for 18 years. The information contained is common to information found in normal search of personal information such as name, address and phone number. Only the section of STARS dedicated to Occupational Health & Safety contains medical cause and treatment information.

5. Expense Management System - Tangoe was the best option to ensure PNS telephone billing requirements could be met. Tangoes 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.

Justice

Description

1. Approximately forty-three (43) employees travelled 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 (http://novascotia.ca/just/IAP/resources.asp).

3. 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 (http://novascotia.ca/just/IAP/resources.asp).

4. 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 (http://novascotia.ca/just/IAP/resources.asp).

5. 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 (http://novascotia.ca/just/IAP/resources.asp).

Conditions

1. Employees are expected to maintain communication with staff at the office and ensure that their BlackBerrys 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 (http://novascotia.ca/just/IAP/resources.asp).

3. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report (http://novascotia.ca/just/IAP/resources.asp).

4. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report (http://novascotia.ca/just/IAP/resources.asp).

5. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report (http://novascotia.ca/just/IAP/resources.asp).

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 (http://novascotia.ca/just/IAP/resources.asp).

3. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report (http://novascotia.ca/just/IAP/resources.asp).

4. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report (http://novascotia.ca/just/IAP/resources.asp).

5. The particulars about the restrictions and conditions can be found in the 2012 PIIDPA Report (http://novascotia.ca/just/IAP/resources.asp).

Labour and Advanced Education

Description

See description of access (or storage) provided in the 2013 annual PIIDPA report http://www.novascotia.ca/just/iap/_docs/piidpa-report-for-minister-2012.pdf.

Conditions

See description of access (or storage) provided in the 2013 annual PIIDPA report http://www.novascotia.ca/just/iap/_docs/piidpa-report-for-minister-2012.pdf.

Reasons

See description of access (or storage) provided in the 2013 annual PIIDPA report http://www.novascotia.ca/just/iap/_docs/piidpa-report-for-minister-2012.pdf.

Municipal Affairs[6]

Description

Ten (10) DMA staff travelled outside Canada during the reporting period on fourteen (14) separate occasions and took their laptop and/or Smart phone while away.

Conditions

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

Reasons

Maintain contact with operations. Authorization to take mobile devices out of country in accordance with the standard provincial authorization process relating to international travel and provincially provided communication devices.

Natural Resources

Description

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

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

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

4. Webex was used for web conferencing.

Conditions

3. Remote access to Outlook is protected by username / password authentication, and is delivered over an SSL-encrypted link via the secure BlackBerry GroupWise server.

---

[6]The Department of Municipal Affairs was established in 2014. The Emergency Management Office reports under the Department of Municipal Affairs.

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

5. 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

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

4. 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.

5. 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.

Office of Planning and Priorities

Description

Three employees took their BlackBerrys out of the country on business trips with the requisite permissions: Iceland, June 6 - 10, 2014 & New York on three occasions: October 10 - 14; November 29 - December I and December 19 – 28; Boston, October 19 - 27, 2014.

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.

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. 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.

Office of Service Nova Scotia[7]

Description

1. Credit card transaction information resulting from payments for online services under the ACOL Contract or for in-person services delivered by SNS 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. Five (5) SNS staff travelled outside Canada during the reporting period on ten (10) separate occasions and took their laptop and/or BlackBerry while away.

3. SNS currently stores approximately 6738 boxes of records with Iron Mountain.

4. SNS 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 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.

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

---

[7] The Office of Service Nova was established in 2014. Report includes Alcohol and Gaming Division.

Reasons

1. SNS 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, SNS took over ownership of the Iron Mountain relationship.

   The Provincial Records Centre will not currently accept any records from SNS that are not backed by STOR and until the STOR has been developed and SNS can find the appropriate funding to transfer the records out of Iron Mountain, SNS 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. 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.

Office of the Premier

Description

1. Two members of the Office of the Premier travelled to South Korea, China, and Boston in August, September, and December of 2014 on government business and had their BlackBerry or other portable devices with them.

Conditions

1. N/A

Reasons

1. In accordance with the PIIDPA, an employee may be permitted to temporarily transport personal information outside of Canada if their Deputy Head considers that the transport is necessary for the performance of their duties. This includes transport of personal information in a cell phone or other electronic device (e.g. BlackBerry). Also under PIIDPA, storage or access of personal information outside of Canada may be permitted by the Deputy Head for transport and, as necessary, the storage or access of personal information while outside Canada.

Transportation and Infrastructure Renewal

Description

1. There were 35 employees who were approved to access their wireless devices when travelling outside Canada in 2014 (see description of access in 2012 annual PIIDPA report http://novascotia.ca/just/IAP/resources.asp).

2. Registry of Motor Vehicles - 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.

3. Registry of Motor Vehicles - 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. See description of access in 2012 annual PIIDPA report. (http://novascotia.ca/just/IAP/resources.asp)

2. Registry of Motor Vehicles - 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.

3. Registry of Motor Vehicles - 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. See description of access in 2012 annual PIIDPA report. (http://novascotia.ca/just/IAP/resources.asp)

2. Registry of Motor Vehicles - 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.

3. Registry of Motor Vehicles - 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.

Foreign Access and Storage by Agencies, Boards & Commissions and Other Public Bodies[8]

Council on African-Canadian Education

Description

A decision was made to allow potential access to personal information via email using devices such as cellphones, iPads, BlackBerrys, and/or laptops in October 2014 while the Executive Director and Chair attended an educational conference in Kansas City, USA.

Conditions

This access was not shared beyond the individuals travelling and was only for the intended purpose of ensuring ongoing operational needs of the Council were met.

Reasons

The decision to allow potential access to personal information outside Canada was for the purpose of ensuring ongoing operational needs of the Council were met while two individuals were away on work-related travel.

Halifax Harbour Bridges[9]

Description

HHB's MACPASS software application maintenance and support is provided by 3M (previously VESystems) primarily located in Austin Texas. 3M provides both routine maintenance and upgrades and have access to personal information through a portal to HHB's internal network. Access is fairly routine and would occur minimally once a month.

Conditions

3M's access is controlled through a secure virtual private network and the services are provided for under the terms set out in an annual service agreement.

Reasons

The MACPASS back office software application is a propriety software application that is critical to HHB and its ability to conduct and operate its electronic toll collection program. The system was purchased in 2008 and has been maintained by its developer since implementation.

---

[8] Elections Nova Scotia, Nova Scotia Provincial Lotteries and Casino Corporation, Nova Scotia Public Service LTD Plan, Office of the Police Complaints Commissioner, RRFB Nova Scotia and Worker's Compensation Appeals Tribunal did not have access or storage outside of Canada to report.

[9] Formerly operated as Halifax-Dartmouth Bridge Commission

Human Rights Commission

Description

Access to personal information through a portal to the organizations internal network via Government-owned BlackBerrys. This occurred during employee travel to three locations through the year: Burlington, Vermont, USA, Wellington and Whanganui, New Zealand, and Leeds, England.

Conditions

Access included voice, data and email.

Reasons

In every instance, the devices were brought out of Canada by a Senior Manager of the Nova Scotia Human Rights Commission while they were on official Commission business. This was necessary because the Commission is a small organization, and access to Senior Officials, even while travelling, was essential to ongoing operations.

In*Nova*corp

Description

1. During the calendar year 2014, there were 10 employees who travelled for business or pleasure and of those 10 employees; there were 15 different acts of access, which included VPN access, BlackBerry access and/or webmail access. Activity occurred within North America.

2. In addition, Innovacorp uses the following during the normal course of business:
   IBM Global Services expense management platform Jan 1,2014-Dec 31, 2014 Expense mgmt
   WebEx Jan 1,2014-Dec 31, 2014 Web conferencing purposes
   Skype Jan 1,2014-Dec 31, 2014 Web conferencing purposes
   Facebook Jan 1,2014-Dec 31, 2014 Social marketing purposes
   Twitter Jan 1,2014-Dec 31, 2014 Social Marketing purposes
   Slimtimer Jan 1, 2014-Dec 31, 2014 On line tracking purposes
   DealFlow Jan 1, 2014-Dec 31, 2014 On-line deal management tool
   DropBox Jan 1, 2014- Dec 31, 2014 On-line file storage tool

Conditions

1. VPN, BlackBerry and/or webmail access usage is password protected either through an individualized password or a company set password. Both types of passwords are changed on a regular schedule.

2. Other items listed above require individual password sets are and changed on a regular basis.

Reasons

1. For business continuity and maintenance, Innovacorp senior management and other key staff must be able to store and access information using various mobile and electronic devices, as long as there is reasonable and direct connection to the person's job duties while travelling outside Canada.

Film and Creative Industries Nova Scotia

Description

1. Approximately five representatives travelled 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

N/A

Reasons

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

Nova Scotia Business Inc.

Description

1. salesforce.com, inc. — CRM data services — storage and access — client / partner / service provider representatives' personal information (primarily business contact information)
   Pursuant to s. 5(2) PIIDPA the head of Nova Scotia Business Inc. (NSBI) determined the storage / access outside Canada of individuals' business contact information in NSBI's custody / control, as part of customer relationship management (CRM) data services supplied under contract by salesforce.com, inc. (a Delaware, US corporation with its principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.

2. VerticalResponse, Inc. — email campaign management services — storage and access — individuals' business contact information (primarily email addresses)
   Pursuant to s. 5(2) PI/DPA the head of Nova Scotia Business Inc. (NSBI) determined the storage / access outside Canada of individuals' business contact information (primarily email addresses) in NSBI's custody / control, as part of email campaign management services supplied under contract by VerticalResponse, Inc. (a US corporation with its principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.

3. TinderBox Inc. — sales proposal management services — storage and access — prospective client representative's business contact information (name, email address) and proposal interaction analytics
   Pursuant to s. 5(2) PIIDPA the head of Nova Scotia Business Inc. (NSBI) determined the storage / access outside Canada of individuals' business contact information (name, email addresses) and proposal interaction analytics information in NSBI's custody /control, as part of the sales proposal management services supplied under contract by TinderBox Inc. (a US corporation based out of Indianapolis, Indiana) is to meet the necessary requirements of NSBI's operation.

4. International in-market consultants — trade development & investment attraction services storage and access — client / partner / service provider representatives' personal information (primarily business contact information)
   Pursuant to s. 5(2) PIIDPA the head of NSBI determined the storage / access outside Canada of personal information (primarily business contact information) in NSBI's custody / control, as part of the investment attraction and trade development services supplied under contract by international in-market consultants (global) is to meet the necessary requirements of NSBI's operation.

5. NSBI directors, officers, employees — performance of duties during international travel — storage and access — personal information
   Pursuant to s. 5(2) PIIDPA the head of NSBI determined the storage I access outside Canada of personal information in NSBI's custody / control, stored in, or accessed using, a mobile electronic device by an NSBI director, officer or employee for business continuity purposes during international travel, is to meet the necessary requirements of NSBI's operation

Conditions

1. salesforce.com, inc. — CRM data services — storage and access — client / partner / service provider representatives' personal information (primarily business contact information)
   The individuals' business contact information is to be protected in accordance with the salesforce.com, inc. master agreement and privacy statement which recognize NSBI as owner of the stored data and provide strong privacy protection and security processes. The service is certified as a "Safe Harbour" under the EU Directive on Data Privacy and is certified "TRUSTe" privacy compliant.

2. VerticalResponse, Inc. — email campaign management services — storage and access — individuals' business contact information (primarily email addresses)
   The individuals' business contact information (primarily email addresses) is to be protected in accordance with the VerticalResponse, Inc. terms of service, privacy statement and anti-spam policy which recognize NSBI as owner of the stored data, provide strong privacy protection and security processes and is US CAN-SPAM Act compliant.

3. TinderBox Inc. — sales proposal management services — storage and access — prospective client representative's business contact information (name, email address) and proposal interaction analytics
   The individuals' business contact information (name, email address) and proposal interaction analytics is to be protected in accordance with the TinderBox Inc. service agreement, privacy policy and security statement which recognize NSBI as owner of the stored data, provides strong privacy protection and security processes and is EU Safe Harbour compliant.

4. International in-market consultants — trade development & investment attraction services — storage and access — client / partner / service provider representatives' personal information (primarily business contact information)
   The personal information (primarily business contact information) is to be protected in accordance with the service agreement including confidentiality provisions.

5. NSBI directors, officers, employees — performance of duties during international travel — storage and access — personal information Personal information stored in or accessed using a mobile electronic device by an NSBI director, officer or employee during international travel is to have a reasonable and direct connection to the person's job duties and be protected by the director, officer or employee in accordance with the NSBI Code of Conduct and Oath of Office and the NSBI Privacy Policy.

Reasons

1. salesforce.com, inc. — CRM data services — storage and access — client / partner / service provider representatives' personal information (primarily business contact information)
   NSBI requires a robust and secure CRM platform to store and manage information necessary for the conduct of NSBI's relationships with its clients, prospective clients, partners and stakeholders. The Salesforce® data service was selected through independent evaluation and based on its superior standing in meeting predefined objective evaluation criteria (including service functionality, IT compatibility, data security, vendor experience and cost). The tangible risk of compromising these critical service requirements outweighs the remote risk of business contact information (given its more accessible public nature) being the target of a foreign demand for disclosure.

2. VerticalResponse, Inc. — email campaign management services — storage and access — individuals' business contact information (primarily email addresses)
   NSBI requires a secure anti-spam compliant email campaign management service that can be integrated with its Salesforce.com CRM service for conducting notification to all or segments of its contacts about events, activities, services of interest to those persons. Domestic suppliers currently do not meet NSBI's technical and service requirements.

3. TinderBox Inc. — sales proposal management services — storage and access — prospective client representative's business contact information (name, email address) and proposal interaction analytics NSBI requires a convenient and secure proposal management service for streamlining the creation, management, customization of NSBI sales proposals, value proposition and program / service promotional presentations for prospective business clients, that can be integrated with NSBI's Salesforce.com CRM service.

4. International in-market consultants — trade development & investment attraction services — storage and access — client / partner / service provider representatives' personal information (primarily business contact information)
   NSBI engages international in-market consultants as an essential and integral component of NSBI's trade development and investment attraction activities. The consultants are experts in the business environment within a business sector or geographic region of interest. International consultants operate from and travel outside Canada and must be able to store and access personal information (primarily business contact information) outside Canada in order to facilitate business connections / transactions in performing their contracted services.

5. NSBI directors, officers, employees — performance of duties during international travel — storage and access — personal information

For business continuity purposes, NSBI directors, officers, employees must be able to store and access, using a mobile electronic device, personal information that has a reasonable and direct connection to the person's job duties so the person can perform work responsibilities while travelling outside Canada.

Nova Scotia Legal Aid Commission

Description

All data is stored in Canada. No data is stored outside of our NS Legal Aid servers. Access can be acquired from anywhere in the world by our employees, but only with a VPN/password-protected phone. Access is only granted to employees. The total number of employees travelling for work purposes with mobile devices would not exceed 25.

Conditions

Restrictions on access are: only by employees with passwords. Access granted to employees only.

Reasons

Access is necessary by our employees to remain in contact with head office and their individual offices for business reasons when travelling. Storage is only in-house.

Nova Scotia Liquor Corporation

Description

No additional decisions were made during the 2014 calendar year to change the way the NSLC stores information outside of Canada. The current arrangement remains in place.

Conditions

All data accessed outside of Canada is secure and encrypted.

Reasons

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

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 two instances where employees travelled 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.

Public Prosecution Service

Description

1. There was no storage of personal information outside Canada by the Public Prosecution Service.There was access to personal information using wireless data devices including BlackBerry and laptops by (15 individuals) on a daily basis while visiting outside of Canada.

Conditions

1. The conditions placed on such access involved the use of encryption and password protection. The BlackBerry was kept in the custody of person during all times.

Reasons

1. The BlackBerry was password protected and was necessary to check for work related messages. Messages received were responded to and staff given directions as requested in a timely manner.

Public Service Commission

Description

1. 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. 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. 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 28 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.

Serious Incident Response Team (SIRT)

Description

The Director of the Serious Incident Response Team travelled outside of Canada with a BlackBerry and laptop that contained personal information (work related). This happened on two occasions during 2014 when the employee travelled on person vacation time.

Conditions

Authorization for travel with these electronic devices was received from the Deputy Minister and was in keeping with government policy and protocol.

Reasons

The Director is required to have his BlackBerry and laptop with him as he is the only person who can authorize an investigation and/or the laying of charges. He is also responsible for the approval of any media releases.

Trade Centre Ltd.

Description

The ticketing system used by Ticket Atlantic is hosted in Irvine California, USA by Paciolan. The data is housed in their managed facility on their AS6000 mainframe computers. Secure access is provided from TCL facilities to the data centre via a secured VPN tunnel. This is data required for the sale and purchase of event tickets from Ticket Atlantic Box Office and is under ownership of TCL.

Conditions

Only use the collected customer information solely for the purposes contemplated in this agreement and otherwise in compliance with all applicable federal and state laws. (The) Customer will own all Personal Information, data and related information collected or received through use of the System by it, or directly by Paciolan, and all compilations thereof, in connection with the operation of the system. Data is stored to ensure we can reconcile delivery of tickets, returns, discrepancies and payment verification to the customer. Customers are asked if they wish to receive future information on events etc. and only then will they be sent any correspondence outside the ticket purchase for which the information was supplied. Other accounts are set up by the customer to purchase tickets online and are maintained for the customer so she/he can purchase tickets online by signing into her/his TA account.

Reasons

In 2004, a tendering process was undertaken to purchase a new ticketing system. Paciolan was chosen as the bid winner as they could offer the best solution for our requirements. No vendor based in Canada could provide the same level of service necessary for our business. The software vendor only offers a hosted business model - the system is not available to be installed on premises. The contract has been extended for an additional two years ending on May 31, 2017. Legal counsel was sought on the original agreement and on the renewal in regard to best practices and privacy requirements and he contract was found to be sound.

Waterfront Development

Description

There were instances when staff travelled outside Canada and took Waterfront Development owned devices such as iPhones and/or laptops and may have accessed personal information.

Conditions

Remote access to email is protected by username/password authentication. All iPhones and laptops must be password protected.

Reasons

When staff travel for business, they are required to monitor their email and voicemail for business continuity and operational purposes.

Workers' Compensation Board of Nova Scotia

Description

1. Employee access to personal information by mobile device (iPhone, iPad, BlackBerry) or computer (laptop, desktop)
   50 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
   686 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
   22 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
   30 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

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

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.

Foreign Access and Storage by District Health Authorities and Provincial Health Care[10]

Annapolis Valley District Health Authority

Description

Approximately 5 AVH employees travelled outside Canada in 2014 who may have accessed their NS health email, BlackBerrys, laptops or other electronic devices containing personal information. No new service contracts were entered into that allowed or required access or storage of personal information outside Canada.

Conditions

Any restrictions or conditions are as provided in the 2012 PIIDPA Annual Report. (http://novascotia.ca/just/IAP/resources.asp)

Reasons

Statement as provided in the 2012 PIIDPA Annual Report. (http://novascotia.ca/just/IAP/resources.asp)

Cape Breton District Health Authority

Description

A total of 6 employees travelled outside Canada and may have accessed email with their BlackBerrys or notebooks. See description of access or storage provided in the 2013 annual PIIDPA report (http://novascotia.ca/just/IAP/resources.asp).

Conditions

See description of access or storage provided in the 2013 annual PIIDPA report. (http://novascotia.ca/just/IAP/resources.asp)

Reasons

See description of access or storage provided in the 2013 annual PIIDPA report. (http://novascotia.ca/just/IAP/resources.asp)

---

[10] Colchester East Hants Health Authority and South Shore District Health Authority did not have access or storage outside of Canada to report.

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.

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.

   Guidelines will be developed related to access and storage of personal information outside of Canada once the regulations are released by the Department of Justice.

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.

2. Specific criteria related to reporting on decisions of access and storage of information from outside of Canada will be developed following the release of regulations by the Department of Justice.

Guysborough Antigonish Strait Health Authority

Description

One Manager travelled outside of Canada with their BlackBerry device and accessed emails. One Radiologist accessed Provincial IMPAX Servers from the United States on one day to read radiology images while on call for Guysborough Antigonish Strait Health Authority.

Conditions

Directors/Managers are required to respond to emails to fulfill employment obligations while maintaining privacy and confidentiality according to the districts' privacy policies and procedures. The radiologists provided radiological interpretation of images in the course of providing patient care. Access to the Web Based PACS system is secure requiring a unique username and password. PACS is a Picture and Communication System for medical imaging.

Reasons

Electronic Devices carried by staff outside of Canada are password protected. Access to patient information by the radiologist was necessary for patient care delivery for the brief time he was outside of Canada.

IWK Health Centre

Description

1. Laboratory Testing - IWK's Department of Pathology and Laboratory Medicine (DPLM) refers some testing to laboratories outside of Canada if specialized testing services are not offered in Canada or if the cost to conduct the testing in Canada is prohibitive. IWK seeks referral laboratories in the USA first, and then internationally. Additionally, referral testing may be required for confirmation of a disease or diagnosis by specialized testing services based on results obtained by IWK laboratories. During the 2014 calendar year, IWK worked with 85 American laboratories, 40 international and 55 Canadian laboratories.

2. Non-Canadian Contractors/Vendors with Remote Access - IWK contracts with some specialized service providers who, in the course of providing their services, remotely access or store personal information in the custody and control of IWK outside Canada. 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). 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); GE Healthcare: United Kingdom (ultrasound system); and Perklin Elmer: Akron Ohio USA (Newborn Screening Program/SpecimenGate application).

3. Business Travel - IWK's records indicate that during the 2014 calendar year, there were approximately 154 incidents of travel booked through the IWK for work-related travel outside of Canada, by 129 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 this travel. Mobile devices, including laptops and cell phones, are generally used for email and/or telephone access while staff are travelling 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 referral laboratories outside of Canada. IWK refers specimens to genetic referral laboratories in accordance with guidelines established by the American College of Medical Genetics (AMCG) and Canadian College of Medical Geneticists (CCMG). Further, IWK refers to laboratories that meet conditions of international and national regulatory organizations, including International Standard ISO 15189, Medical Laboratories "Particular Requirements

for Quality and Competence. ISO 15189 addresses the selection, assessment and monitoring of the referral laboratories and confidentiality requirements. Laboratories that do not meet these conditions may be used at the discretion of the clinician and care team if deemed appropriate and necessary. All referrals are tracked by two laboratory information systems, (LIS) Meditech and Shire Management System (SMS). Any new IT/electronic medium used to facilitate referral services has a Privacy Impact Assessment completed prior to use.

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, 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). When dealing with large vendors, Site-to-Site VPN access can be used. IWK's Department of Biomedical Engineering scrubs/destroys all personal information stored on equipment when sent outside the Health Centre for repair or servicing. 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. As an example, access to Survey Monkey, a web-based surveying tool, is restricted on IWK's network. Data input into Survey Monkey is stored outside Canada, as its server is located outside of Canada. 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 staff on May 1, 2009. Access remains restricted 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 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 have encryption software and are password protected. IWK handheld electronic devices 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 email is not accessible, while still allowing the telephone capabilities 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 allows IWK network administrators to control what users can do when accessing the IWK network remotely. Certain functions are controlled or prevented, e.g.: copy/paste, remote printing and mapping of serial and printer ports. This software turns a remote access session into a 'window' capable of viewing IWK systems, but prevents information from being removed from the system. IWK BlackBerrys and staff phones are mandatorily password protected. Non-use of the device for five minutes triggers the user 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 use 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. Genetic testing is an evolving field continually requiring increasingly esoteric testing. IWK provides genetic testing for the Maritime Provinces, and required testing sometimes is cost prohibitive to obtain in Canada or is not available in Canada at all, necessitating international referrals.

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 for the purpose of ongoing patient care or research.

Merged Services Nova Scotia[11]

Description

Storage of personal information outside Canada was not permitted in the above-noted calendar year. However, on 24 different occasions, personal information was permitted to be accessed outside Canada by HITS-NS staff in order to provide operational assistance for applications supported by HITS-NS as agents for various custodians (Department of Health and Wellness, each District Health Authority, the IWK Health Centre, and private physicians). As well, further to direction from the Department of Health and Wellness, support vendors for systems supported by HITS-NS including the NShIS and SHARe which are US-based were allowed to access systems in order to provide operational support, the details of which are contained within the Department's report.

Conditions

Personal information was only accessed using HITS-NS-owned devices (BlackBerrys and laptop computers), which require passwords and encrypt all information contained thereon. Personal information accessed by vendors was done by means of a secure Virtual Private Network.

[11] Previously reported under the Department of Health and Wellness.

Reasons

As the body tasked with supporting critical healthcare systems in the Province of Nova Scotia, at times this requires access to the systems to be allowed outside of Canada when staff are travelling outside the country.

Pictou County Health Authority

Description

Eighteen (18) individual release of information requests were completed and sent to the United States. One release of information request was completed and sent to Scotland. In each instance, consent was received prior to completing the release of personal health information. The CEO (Mr. Pat Lee) brought his BlackBerry and laptop on a work related trip to Indonesia.

Conditions

Staff are not allowed to bring their cellular devices or laptops out of country without prior approval. Staff only use HITSNS and PCHA approved electronic storage for all electronic information. There are no unapproved releases of information completed without proper signed consent.

Reasons

As per the Personal Health Information Act (PHIA), any release of information request completed required appropriate consent prior to release. PCHA does not store any electronic information on servers outside of the country; if a request was made it would go through a review process to determine the risk and availability of other potential options/solutions.

South West District Health Authority

Description

In 2014 there were 4 SWH employees involved in international trips where they maintained access to the organization through BlackBerrys, laptop remotely through VPN. There were no new systems/service agreements in 2014 the list would be the same as in 2013.

Conditions

The district continues to add the inclusion clause re the management of the information in all requests for proposals, new contracts, warranties or renewals. The Proponent acknowledges that the Districts are bound by the terms of the Personal Health Information Act, S.N.S. 2010, c.41 ('PHIA'), the Freedom of Information and Protection of Privacy Act, S.N.S. 1993, c. 5 ('FOIPOP'), the Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3 ('PIIDPA') and the Privacy Review Officer Act, S.N.S 2008, c.42.

Reasons

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

Foreign Access and Storage by Universities and Colleges[12]

Cape Breton University

Description

1. Alumni/Donor Database: CBU uses software provided by an American vendor, Blackbaud, located in South Carolina. Although the system originates from the SU, 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 a distance program. As well, student have web access to the Student Information System to view their individual financial and academic records.

3. Course Management System: CBU used 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 has implemented StarRez, a Residence Management System provided through StarRez Inc. from Greenwood Villages, Colorado. 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 sites 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. SchoolDude: SchoolDude is a cloud-based ticket tracking system used by CBU's Facilities Management Department. The SchoolDude data centre is located in the US and in some cases offshore storage is also used. Personal data stored in this system is restricted to CBU faculty and staff information available on CBU's public website www.cbu.ca.

7. BaseCamp: This project management system is used by CBU's Marketing and Communications group. The personal data being stored in this US-based cloud system is limited to CBU staff information that is publicly available on our website.

---

[12] Atlantic School of Theology did not have access or storage outside of Canada to report. Acadia University did not provide a completed PIIDPA Form 1.

8. Hubspot: HubSpot is an inbound marketing and sales software platform used by the CBU Marketing and Communications Department. HubSpot has offices in Cambridge, Mass.; Dublin, Ireland; and Sydney, Australia. Personal information of CBU contacts and prospective and current systems are held in HubSpot's cloud-based data centres outside Canada. The Marketing and Communications Department has determined that no Canadian solution exists that will provide the functionality of HubSpot, and that use of the system is necessary to the operations of the Department.

9. Travel: CBU faculty and staff participated in 42 international trips to 18 different countries in 2014. Employees have web access to their personal email via smart phone, tablet or laptop. Some would also have 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

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

2. Storage of personal information outside Canada (HubSpot). CBU informs individuals, prior to collecting any information that their information is stored outside Canada and what measures are taken by CBU in addition to the third-party provider to protect privacy and confidentiality, including that information will be collected and used only for its specified purpose. CBU obtains an individual's consent before collecting any information; a user's information, for example name and email address, is provided voluntarily for this purpose. A confirmation email is sent from CBU to the user containing instructions on how to unsubscribe from the service which removes the user's information from the database. The information is password protected, and CBU has the capacity to download the information and delete the account if necessary.

Reasons

1. Access: For access to the Raisers Edge and the StarRez systems, these American-developed products were determined to be the best fit for CBU needs, and are widely used in Canada. Access by these firms is restricted as described above. With respect to access by CBU employees travelling outside the country, such access is necessary for university administrators, researchers, and other employees to perform their assigned duties.

2. Storage: The user Department (Marketing and Communications) has determined that security and privacy provided by HubSpot meets the needs of the University, and no Canadian solution could provide the required functionality. The President of the University is in agreement that the use of the system is a necessary requirement of the operation.

Dalhousie University[13]

Description

1. Online Exam Preparation. Exam preparation tool for BScN students (Storage in United States).

2. Event Registration Management Tool: Technical Support for event registration and professional development software. (Remote access from US).

3. For items 3 through 6 see corresponding descriptions of access or storage provided in the 2013 annual PIIDPA report: 3.Online Communications and Collaboration Tools; 4.Athletics Schedules and Scores; 5.Academic Instructional Tools; and6.College Student Inventory (CSI). For items 7 through 33 see corresponding descriptions of access or storage provided in the 2012 annual PIIDPA report: 7.Financial Services Electronic Forms; 8.University ID Card; 9.Network and Systems Upgrades; 10.Wireless Products; 11.Apple Warranty Maintenance; 12.Teaching and Research Statistical Software; 13.Collaborative Teaching Software; 14.Service Provider Maintenance (IBM Hardware and Software); 15. Administrative Computing Software; 16.Room Reservations Software; 17.Degree Progress Software; 18.Student Advising Scheduling Software; 19.Student Performance and Referral Software; 20.Medical Education Evaluations Software; 21.Dentistry Academic Materials Software; 22.Service Provider Maintenance (Xerox Hardware and Software); 23.Website Feedback; 24.Plagiarism Detection; 25.Clinical Experience Software; 26.Law Student Survey; 27.Undergraduate Student Survey; 28.Crowd Sourcing Product; 29.Hosted Learning Management System; 30.Student Learning Outcomes Software; 31. Environmental Health & Safety Database; and 32.Online Law School Exams. For item 33 see corresponding descriptions of access or storage provided in the 2006 annual PIIDPA report; 33.Employee Temporary Remote Access.

Conditions

1. Online Exam Preparation: Contractual obligations on service provider to take precautions to maintain confidentiality of the data and not use, distribute or disclose the data for unauthorized purposes. University provides access to the software and students provide limited personal information, with ability to utilize alias if desired (no personal information necessary).

2. Event Registration Management Tool: Limited access only where required for maintenance and troubleshooting. Contractual security measures including restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to University protocols including time restrictions, audit function, pre-approved IP addresses, and additional measures deemed appropriate by Dalhousie.

3. As per above.

---

[13] Report includes the Nova Scotia Agricultural College.

Reasons

1. Online Exam Preparation: Change to national licensure examination resulting in BScN students now being required to write US based national licensure examination beginning in 2015. Key aspect of curriculum /exam preparation with no Canadian equivalent.

2. Event Registration Management Tool: Essential to ongoing needs of the University with respect event management registration (conferences, workshops, symposia, etc.) and professional development. Superior range of service and functionality; previous university experience with service provider offerings resulting in integration with existing systems; allows for self-registration and management.

3. As per above.

Mount Saint Vincent University

Description

We did not store any information such as employee data, student records, or other personal information outside Canada.

Access from Outside Canada: Students, faculty and staff (whether travelling or living) outside Canada were granted access to email accounts and information systems stored on servers within Mount Saint Vincent University (and within Canada) *via* email or remote access systems, using appropriate authentication credentials.

Conditions

There was no limit on the amount of information that a student, faculty or staff member could access from outside Canada within their access rights. The information they have access to is maintained on a server controlled by Mount Saint Vincent University (within Canada).

Reasons

Access to information (from outside Canada) is necessary for students to complete their course work and for faculty and staff to complete their work assignments and/or research. Decisions to allow students to access their course material and relevant data are maintained within the Distance Learning and Continuing Education department and the course/instructor level. Faculty and staff remote access to Mount servers and systems are the responsibility of the department chairpersons or department managers with consultation from Information and Technology and Services.

Storage of personal information or data is not currently housed outside of Canada, however any decisions on future hosting of personal information such as Student Email, would need the approval by the Senior Executive Team including the President of the University. As the University must maintain full control of all its data, at all times, any system that the University would consider, in the

future, to host information outside of Canada would need to provide significant reduction in costs, administration or increased functionality while providing, at minimum, the same security controls and procedures to protect the University's data.

Nova Scotia College of Art and Design

Description

All Enterprise databases containing personal information are carefully monitored and remain in Canada. Access to personal data from outside Canada is granted in certain circumstances.

1. There are 2 employees who travel internationally and may use a smart phone, laptop or other electronic device to authenticate to our system and access personal information.

2. Trained vendor technologists from a U.S. vendor are permitted access during necessary support sessions.

3. In May, 2014, NSCAD University authorized the use of Office 365 for a large number of its employees, including email, user storage and collaboration tools. Since these email and storage servers could be located on foreign soil, it is possible that personal information could inadvertently be stored on those servers.

Conditions

NSCAD University has taken a number of steps to restrict or limit access to personal information from outside Canada.

1. In the case of authorized access by employees, the access requires secure authentication and unnecessary access is denied by application security.

2. In the case of vendor support sessions, the sessions must be expressly permitted by the Director, Computer Services and attended by an employee approved by the Director, Computer Services

3. With regards to Office 365, it was discovered that employees were already using foreign-based email services (eg. Gmail) and foreign-based storage services (eg. Dropbox) to facilitate their work. The University investigated and decided that in the absence of a viable and affordable Canadian competitor, it would at least be appropriate to promote more secure and cost-effective solutions in the interim. Our perceived best practice in the industry is to provide and promote Microsoft Office 365 services. NSCAD University adjusted policies and provides employee training sessions to prohibit the non-essential disclosure of personal information.

Reasons

In all cases we feel our actions to be necessary.

1. International travel, different time zones and the service of International student applicants makes access to the information systems that serve these groups necessary. NSCAD feels

this access prevents less secure transfer methods such as email, computer file or paper-bases transfers.

2. Expert support for our ERP system is only available from our Vendor. NSCAD uses Canadian industry standard software in this regard.

3. The use of vendor-supplied, Cloud-based services such as email and file storage is quickly becoming best practice because of the efficiency, cost-effectiveness and superior security. In the past NSCAD and other Universities have struggled to keep up with the latest software versions, security patches and news releases necessary to protect information. Using vendor-supplied software ensures our security is current. NSCAD continues to work with other Universities and Industry partners to improve and ensure it is following Industry best practices.

Nova Scotia Community College

Description

As required by section 5(3) of the Personal Information International Disclosure Protection Act (PIIDPA) 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 online 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. The College no longer qualifies for the grandfathering provisions provided by the Act. Since our last submission (March 10, 2014), the College has launched an in-house online application system which has been built in our PeopleSoft ERP. This was launched in July 2014 and the prior vendor hosted interface Apply Yourself was decommissioned on July 31, 2014. As a result, all data is now held in-house within our College ERP. As required by the Act, I would also like to inform you that:

1. 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.

2. 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.

3. The College has seen increased usage of consumer based cloud offerings, such as Dropbox and OneDrive, on our networks. The College doesn't promote the usage but it can't stop it. The College is in the early planning stages to provide secure local based services as an alternative.

Conditions

See above

Reasons

See above

St. Francis Xavier

Description

1. The University's financial software 'Bi-Tech' is provided by a U.S. software vendor Sungard Bi-Tech since 1988. The software requires periodic maintenance and updates. These maintenance needs and updates are applied to our financial software through remote access link between our 'Bitech' server located in Chico, California. The access to our server is for software maintenance only. It is theoretically possible that personal information could be accessed at those times, hence, this notification.

2. Kinetics software (Kx) is a comprehensive software program that manages catering, facility and residential bookings. It is comparable to large conference or hotel management systems. The Conferences and Special Events Department uses the program as our main software to support our operations, making use of the Events, Catering, Marketing and Extracts modules available within the software.

3. After a review of available systems, a decision was made to purchase a web-based application called EZ Facility to help manage the day-to-day business of Campus Recreation. The application allows for improved membership management, point of sale, scheduling, financial and facility reporting, invoicing and intramural sport organization.

4. Due to web support and maintenance expertise that could not be performed in-house, the decision was made to have the StFX.ca website hosted by a US based company called Acquia. The company was selected based upon their expertise with the content management software that StFX.ca was built upon.

5. After reviewing available customer relationship management (CRM) systems, StFX decided to manage student contact information in StFX's custody and control through data services supplied under contract by salesforce.com inc. Salesforce.com are a US company based in Delaware, with its primary place of business in San Francisco, California.

Conditions

1. The University has taken steps to minimize our exposure by restricting access to our system to designated and pre-scheduled time periods and only when maintenance and update activities cannot be accomplished by university personnel. We are working with mature software product and, historically, access has been for semi-annual updates only, therefore, we have minimal exposure points.

2. Vendor provides technical support through remote access, previously arranged with the university technology support group for each incident.

3. The following data is stored in the system: member name, date of birth, address, membership type, membership start and end date, purchases made, time and date of facility entry. Credit cards are not stored in the system and no banking transactions are completed within the system. Anyone set up with a user account has access to data based on role and permission settings. Access is limited to need of role.

4. Collected information is stored on the Acquia.com servers for a short period until St. FX employees download and delete the information housed in Acquia. Employees log in to servers with user names and passwords and, thus, this information passes through the servers but is managed and stored within servers at St. FX not on Acquia.com servers.

5. The contact information is to be protected in accordance with the salesforce.com inc master agreement and privacy statement which recognize StFX as owner of the stored data and provide strong privacy protection and security processes. The service is certified as a 'Safe Harbour' under the EU Directive on Data Privacy and is certified 'TRUSTe' privacy compliant.

Reasons

1. The cost of switching our software vendors is cost prohibitive at this time and Bi-Tech provides the support required for efficient and secure operation.

2. The only method of receiving technical support is through remote access by the vendor.

3. Data for our EZ Facility account is stored and managed within the Rackspace Data Centers in the US.. Both Rackspace and EZ Facility are PCI Level 1 certified (highest possible), which is the Payment Card Industries global standard for data security. This involves tracking and permission limits to accessing account data and personal information. Hosting an application on our own servers was not a viable option at the time of purchase (and is still not).

4. The technical expertise to host and support StFX.ca content management system was found with the named company and not found within Canada.

5. As competition for both domestic and international students intensifies StFX requires a robust and secure CRM platform to store and manage information necessary for the conduct of StFX's relationships with its students and prospective students. After a thorough evaluation the Salesforce® data service was selected for its superior ratings on a criteria relevant to StFX's operating environment and needs.

St. Mary's University

Description

1. Plagiarism Detection: See description of access or storage provided in the 2012 annual PIIDPA report (http://novascotia.ca/just/IAP/resources.asp).

2. Maintenance Management System: See description of access or storage provided in the 2012 annual PIIDPA report (http://novascotia.ca/just/IAP/resources.asp).

3. Travel: See description of access or storage provided in the 2012 annual PIIDPA report. (http://novascotia.ca/just/IAP/resources.asp)

4. Facilities Asset Management System: See description of access or storage provided in the 2012 annual PIIDPA report (http://novascotia.ca/just/IAP/resources.asp).

5. Schwab Charitable: This US organization based in San Francisco, CA represents a private donor in the United States 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. Schwab Charitable requires the home addresses, telephone and birthdates for all of the University's Board of Governors as part of their due diligence required for the transfer of funds to international charities.

6. Ruffalo Cody provides hosted, cloud-based call centre software to Saint Mary's University, 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 United States. This data is accessed via a Canadian FTP server.

7. Qualtrics: Qualtrics is a private research software company, based in Provo, Utah which provides online survey software.

8. Saint Mary's University Commercial Card Program: Total System Services, Inc. (TSYS), a U.S. Bank third party service provider, stores the data in the U.S. for the St. Mary's University card program. The University's corporate VISA program supports the efficient processing of high volume / low dollar value transactions. It runs across all departments (both academic and administrative.)

Conditions

1. to 4. see response provided in the 2012 annual PIIDPA report. (http://novascotia.ca/just/IAP/resources.asp)

5. Only for internal use to meet IRS standards.

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

7. No personally identifiable information stored outside of Canada.

8. Only business addresses and employment identifiers are stored on servers in US. U.S. Bank meets all Compliance Attestation from the Payment Card Industry (PCI) Data Security Standards. All Transaction Data is stored in secure data centres located in the USA - which in fact is the case for most of the Canadian banks. Data at rest for mainframe systems is stored with TSYS on encrypted Hitachi Storage Devices (HDS) and IBM Virtual Tape System (VTS) storage hardware. AES-256 encryption is enabled on all HDS and IBM hardware. Encryption used is integrated key management and no external key management is required. Data transmitted on mainframe systems uses Connect-Direct NDM (a third party application). U.S. Bank controls the implementation of encryption for files sent since it owns the network and router connection.

Reasons

1. to 4. see response provided in the 2012 annual PIIDPA report. (http://novascotia.ca/just/IAP/resources.asp)

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

6. 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.

7. We will be storing survey data that will not have any personally identifiable information.

8. All financial institutions running corporate credit card programs use the services of this organization.

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 King's College

Description

1. Alumni/donor database: Raiser's Edge software provided by an American vendor, Blackbaud. Alumni and donor data is hosted by vendor on a Canadian cloud system. Data center is in Vancouver. Vendor provides technical service from time to time via remote access while under the supervision of King's. This product has been determined to be the best fit for King's needs and is widely used in Canada.

2. Conference management software: Conference Programmer software provided by an American vendor, Seattle Technology Group, Inc. Personal information is held in Conference Programmer's cloud-based data centres outside Canada. Essential to ongoing needs of King's with respect to conference services. Superior range of service and functionality; more than 150 university clients. Limited supervised access only where required for maintenance and troubleshooting. King's has determined that security and privacy provided by the vendor meets the needs of the University. Vendor is committed to sharing audit information, customer data is completely segregated, database activity is logged and proper encryption protocols are followed with regard to data in transit, file uploads and data in storage.

3. Maintenance management software: MicroMain software provided by an American vendor, MicroMain Corporation. In 2014 data was stored on a server housed on the Dalhousie University campus. Personal data stored in this system is restricted to King's employees. In 2015 data will be housed in a US-based cloud system.

4. Learning management system: Blackboard, provided by Dalhousie University, contains personal information of students. Because of the integration of many of King's information technology services with Dalhousie, King's makes no representations with respect to any of its information stored on or processed through Dalhousie University servers.

5. Journalism internships: web-based Google Drive Intern Evaluation form is used by Internship Supervisors to provide student internship feedback to faculty. Forms are sent to a Gmail account whereby faculty enter log in credentials to download evaluation forms to a university server.

6. Employee access to personal information from outside of Canada is not permitted unless the employee is using a web-based or other internet access tool as a necessary part of performing his or her assigned duties or as a necessary part of a research project. Employees may transport personal information temporarily outside Canada only to the extent that it is strictly necessary for their assigned duties or as a necessary part of a research project. In such event, employees are required to take all reasonable precautions to protect the personal information. Online access is restricted by the use of proper authentication protocols.

7. To the best of our knowledge, no other storage of personal information exclusively in the custody or under the control of King's occurred during 2014.

Conditions

Access to personal information outside of Canada is limited to authorized personnel. In the case of an external entity requiring access for the purpose of technical support and maintenance, all access is controlled and performed under the supervision of King's staff. If it involves a server housed at Dalhousie University, it would require the approval and supervision of authorized Dalhousie staff.

King's has implemented a privacy policy entitled, "University of King's College Privacy Statement" to address the requirements of the PIIDPA legislation. The policy is circulated annually to all employees. See provisions 11 through 14: http://www.ukings.ca/files/u42/Kings-Privacy-Statement-FINAL.pdf Access and storage of personal information in accordance with the policy is accepted by King's as appropriate.

Reasons

The American-developed software products noted above were determined to be the best fit for King's needs and are widely used in Canada. Access is restricted as described above.

Access to personal information from outside of Canada in the custody or under the control of King's under the privacy 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."

Foreign Access and Storage by School Boards[14]

Annapolis Valley Regional School Board

Description

1. One AVRSB staff member travelled outside Canada for business and had the ability to access personal information contained in email or stored in the Groupwise email system, using a BlackBerry and laptop. Staff must seek permission from the head of the public body before taking devices and personal information across the Canadian border.
2. The AVRSB and several of its schools operate Twitter accounts. Twitter is a social media platform based in the United States. These accounts are used for sharing AVRSB/school news, photos and other information to a broader audience.
3. 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 is being evaluated to measure its impact on achievement, attendance and engagement and identify any successes. Personal information about students and teachers may have been accessed and stored outside Canada as the Khan Academy is located outside Canada.
4. The Annapolis Valley Regional School Board utilizes the Aesop System provided by Frontline Technologies Canada (FTC), which is an automated tool used for tracking, processing and storing information related to employee 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. 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. AVRSB and some of its schools use Twitter to share information and interact online with the public and organizations in social spaces. AVRSB collects no IP addresses or personal

[14] Atlantic Provinces Special Education Authority did not have access or storage outside of Canada to report.

information through these services. AVRSB retweets other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.). When Tweeting about events or news within our region, AVRSB ensures that personal information is not shared, or only shared with permission of the individual.

3. It was recommended that teachers set up Khan Academy student accounts so that students are under the age of 13, which is the minimum age to post comments, change their password, etc. It was 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 was 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 was recommended that teachers delete all Khan Academy student accounts at the end of the pilot, in June, 2014.

4. The Department of Education and Early Childhood Development and the Annapolis Valley 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 AVRSB 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 ISO 9001:2000 certified by Lloyd's Registry Quality Assurance. Employees of Frontline have signed confidentiality agreements with the company. Only personnel authorized by the AVRSB 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. Staff are expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. Use of a BlackBerry was necessary to make calls, access email and Internet sites. Use of a laptop computer was 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. There are no Canadian server alternatives to Twitter.

3. 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.

4. FPT's Aesop system is functionally superior 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.'

Cape Breton-Victoria Regional School Board

Description

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 provider (ASP) model for provision of the system to the School Board. The software and data reside in Toronto, Canada and the company is paid a yearly fee for its usage. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system.

The system is supported and maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA. There are two types of support, technical and end user. Technical support is required to ensure the system is operating as 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.

Approximately eight staff members travelled outside Canada and may have, or had the ability to, access personnel information via remote email, BlackBerry and/or personal computer with permission of the Superintendent.

Conditions

The Department of Education and seven school boards signed a 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 BlackBerrys, iphones and personal computers are password protected.

Reasons

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 an on-site audit of their facility and processes. FTC have signed off on all security and information privacy clauses in the contract, understand and agree to comply with the province's PIIDPA legislation, do not store data in the US, and use secure methods for all data transmissions. Also all data accesses by employees of the parent company (Frontline Placement Technologies) are restricted to specific purposes and logged and reported to DOE monthly.

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.

Travel with electronic devices - Staff are sometimes expected to monitor their email 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.

FURTHER COMMENTS:

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 20ll.pdf.

Chignecto-Central Regional School Board

Description

1. Travel with electronic devices: A number of Chignecto-Central Regional School Board staff travelled 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. Staff seek permission from the head of the public body before taking devices and personal information across the Canadian border.

2. Use of Social Media: (a) Twitter – The CCRSB 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. (b) Facebook – The CCRSB also uses Facebook as a professional communication tool to engage the school community and share relevant information to parents, teachers, students and the public. Facebook is based in the United States.

3. The Chignecto-Central 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. Remote access to staff email accounts through Microsoft Outlook is protected by username/password authentication and is delivered through a combination of VPN and encryption.

2. (a) The CCRSB uses Twitter to share information and interact online with the public and organizations in social spaces. The CCRSB collects no IP addresses or personal information through these services. The CCRSB retweets other government accounts and public safety information from partners (RCMP, municipality, school board, etc.) (b) The Board posts information related to the wider school community and may share other government posts, announcements and/or public safety information from partners. As with Twitter, the Board collects no IP addresses or personal information through these services.

   Photos and videos that are posted to all social media platforms have written consent from the people in them where required.

3. The Department of Education and Early Childhood Development and the Chignecto-Central 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 Chignecto-Central 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. 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. There are no Canadian server alternative to Twitter or Facebook.

3. 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."

Conseil Scolaire Acadien Provincial

Description

1. A number of CSAP staff members travelled 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. The board approved 8 school trips outside Canada for a variety of learning experiences.

2. 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.

3. CSAP operates a Twitter account for sharing government news releases, videos, photos and other information to a broader audience.

4. CSAP and some schools have on-line subscriptions for education media Learning A - Z.

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

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

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

2. See details provided in the 2013 NS annual PIIDPA report under South Shore Regional School Board.

3. Twitter is used to share information and interact online with the public and organizations in social spaces. CSAP 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.

4. See details provided in the 2013 NS annual PIIDPA report under Conseil scolaire acadien provincial (http://novascotia.ca/just/IAP/resources.asp).

5. See details provided in the 2013 NS annual PIIDPA report under Conseil scolaire acadien provincial http://novascotia.ca/just/IAP/resources.asp).

6. See details provided in the 2013 NS annual PIIDPA report under Finance and Treasury Board (http://novascotia.ca/just/IAP/resources.asp).

7. See details provided in the 2013 NS annual PIIDPA report under Education and Early Childhood Development (http://novascotia.ca/just/IAP/resources.asp).

Reasons

1. Staff members 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. Laptops and iPads are needed for preparing documents, and accessing email and Internet sites. Staff members accompanying students are required to have in their possession or the ability to rapidly access personal information in case of emergencies while away.

2. See details provided in the 2013 NS annual PIIDPA report under South Shore Regional School Board (http://novascotia.ca/just/IAP/resources.asp).

3. Social media platforms are used to engage the community, increase public awareness, and to promote the dissemination of accurate, timely information. There are no Canadian server alternatives to Twitter.

4. See details provided in the 2013 NS annual PIIDPA report under Conseil scolaire acadien provincial (http://novascotia.ca/just/IAP/resources.asp).

5. See details provided in the 2013 NS annual PIIDPA report under Conseil scolaire acadien provincial (http://novascotia.ca/just/IAP/resources.asp).

6. See details provided in the 2013 NS annual PIIDPA report under Finance and Treasury Board (http://novascotia.ca/just/IAP/resources.asp).

7. See details provided in the 2013 NS annual PIIDPA report under Education and Early Childhood Development (http://novascotia.ca/just/IAP/resources.asp).

Halifax Regional School Board

Description

1. A total of five (5) Halifax Regional School Board staff travelled outside Canada for business and/or pleasure on six (6) separate occasions, 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, Smart Phones and laptops. Staff seek permission from the head of the public body before taking devices and personal information across the Canadian border.

Conditions

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

Reasons

1. Staff are expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. Smart 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.

South Shore Regional School Board

Description

1. Travel with electronic devices: A number of South Shore Regional School Board staff travelled 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 and personal information across the Canadian border.

2. Use of social media: (a) Twitter - 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. (b) Facebook - The SSRSB also uses Facebook as a professional communication tool to engage the school community and share relevant information to parents, teachers, students and the public. Facebook is based in the United States.

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. There were 24 people. Some travelled a few times, but the number of people was 24.

Conditions

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

2. Social media: (a) 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 board, etc.) (b) The Board posts information related to the wider school community and may share other government posts, announcements and/or public safety information from partners. As with Twitter, the Board collects no IP addresses or personal information through these services.

   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 students are under the age of 13, which is the minimum age to post comments, change their password, etc. 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 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: Social media platforms are used to engage the community, increase public awareness, and to promote the dissemination of accurate, timely information. There are no Canadian server alternatives to Twitter or Facebook. 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.

3. Khan academy: 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.

4. Aesop: FPT's Aesop system is functionally superior 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. Travel with electronic devices - A number of 22 Regional School Board staff travelled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in the Board's Lotus Notes 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. The Head of the Public Body provided permission for one employee to take a Board owned device for the Nova Scotia International Student Program. The employee travelled with a group of students and it was necessary to have connectivity with parents and supervisors. It was also necessary for the Head of the Public Body to take an iPhone while travelling to the United States to maintain immediate contact with Board Operations.

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 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.

3. Use of Social Media: (a)Twitter - The Strait 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. (b)Facebook - Several schools within the Strait Regional School Board also use Facebook as a professional communication tool to engage the school community and share relevant information to parents, teachers, students and the public. Facebook is based in the United States.

Conditions

1. Remote access to staff email accounts through Lotus Notes 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 (xxx) 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 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. (a)The Strait Regional School Board uses Twitter to share information and interact online with the public and organizations in social spaces. The SRSB collects no IP addresses or personal information through these services. The SRSB retweets other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.) (b) The Board posts information related to the wider school community and may share other government posts, announcements and/or public safety information from partners. As with Twitter, the Board collects no IP addresses or personal information through these services. 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 and iPhones 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 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. Social media platforms are used to engage the community, increase public awareness, and to promote the dissemination of accurate, timely information. There are no Canadian server alternatives to Twitter or Facebook.

Tri-County District School Board

Description

1. A number of the Tri-County Regional School Board staff travelled 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 and personal information across the Canadian border.

2. Twitter - Some schools within the Tri-County Regional School Board operate 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. Facebook - Some of the Tri-County Regional School Board schools also use Facebook as a professional communication tool to engage the school community and share relevant information to parents, teachers, students and the public. Facebook is based in the United States.

4. 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.

5. The Tri-County 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.

6. The Tri-County Regional School Board utilizes PowerSchool, which is an online student information system, the servers for which are housed in Halifax.

7. Aesop - The Tri-County 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. Remote access to staff email accounts through Microsoft Outlook is protected by username/password authentication and is delivered through a combination of VPN and encryption.

2. The Tri-County Regional School Board schools use Twitter to share information and interact online with the public and organizations in social spaces. The Tri-County Regional School Board collects no IP addresses or personal information through these services. The schools retweet other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.)

3. The Board posts information related to the wider school community and may share other government posts, announcements and/or public safety information from partners. As with Twitter, the Board collects no IP addresses or personal information through these services. Photos and videos that are posted to all social media platforms have written consent from the people in them where required.

4. It is recommended that teachers set up Khan Academy student accounts so that students are under the age of 13, which is the minimum age to post comments, change their password, etc. 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.

5. The Department of Education and Early Childhood Development and the Tri-County 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 Tri-County 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.

6. On occasions when technical support or trouble shooting may be required, Pearson headquarters is based out of the United States. Pearson could be accessing data from our Canadian databases, while in the United States.

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. There are no Canadian server alternatives to Twitter or Facebook.

3. Social media platforms are used to engage the community, increase public awareness, and to promote the dissemination of accurate, timely information. There are no Canadian server alternatives to Twitter or Facebook.

4. 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.

5. FPT's Aesop system is functionally superior 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.

6. All Nova Scotia schools are using PowerSchool. The Province wanted to go with a provincial standard platform, and PowerSchool met all the requirements and was the product selected in the end.

Foreign Access and Storage by Municipalities[15]

Cape Breton Regional Municipality

Description

Several employees from the CBRM travelled outside the country with their mobile devices including cell phones, iPads, and laptops. Many of the devices contained municipal email and were connected to the CBRM instance of Exchange. It was necessary for these employees to be able to communicate with CBRM while away. The Director of each department approved staff members' use of mobile devices while out of the country.

Conditions

The CBRM does not store any information outside Canada. With respect to mobile device use, there were no specific restrictions placed on the mobile devices but does require CBRM network authentication to connect.

Reasons

The current practice has been long standing with the CBRM. The CBRM is in the process of reviewing these practices and formulating more secure policies.

---

[15] Cumberland Joint Services Management Authority, Halifax Public Library, Municipality of the County of Annapolis, Municipality of the County of Antigonish, Municipality of the County of Cumberland, Municipality of the County of Inverness, Municipality of the District of Argyle, Municipality of the District of Barrington, Municipality of the District of Clare, Municipality of the District of Digby, Municipality of the District of St. Mary's, Municipality of the District of Shelburne, Region of Queens Municipality, Town of Antigonish, Town of Hantsport, Town of Lockeport, Town of Mahone Bay, Town of Oxford, Town of Parrsboro, Town of Pictou, Town of Shelburne, Town of Stellarton, Town of Stewiacke, Town of Trenton, Town of Westville, Town of Windsor, Town of Yarmouth and the Municipality of the District of Shelburne (Joint Services Board) did not have access or storage outside of Canada to report. Digby Area Recreation Commission, Municipality of the County of Kings, Municipality of the County of Victoria, Municipality of the District of Lunenburg, Pictou County District Planning Commission, South Shore Regional Library Board, Town of Berwick, Town of Clark's Harbour, Town of Kentville, Town of Mulgrave, Town of Port Hawkesbury and Windsor-West Hants Planning did not provide a completed PIIDPA Form 1.

Halifax Regional Municipality[16]

Description

1. Between January 1st and December 31st, 2014, forty-eight (48) HRM staff and six (6) 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.

2. 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.

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.

4. GIRO (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.

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.

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

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.

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.

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. 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.

---

[16] Report includes Halifax Regional Police

11. Trapezes (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. 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.

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 applicable production systems for support and maintenance purposes.

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. Nashco Consulting Limited, with regional offices in Cochran, Alberta and San Diego, California were provided access on an approved, need basis to the ServiceNow development and production environments for support and enhancement 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 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.

24. Service Providers - Desire2Learn - Brightspace, Learning Management System, with a headquarters in Kitchener, ON.

25. Xerox Corporation (Print Services), with an American headquarters in Norwalk, CT were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

Conditions

1. Prior to travelling, staff were advised that HRM Communication tools (Cell Phones, BlackBerrys, Laptops, Memory Sticks, VPN) were to be password protected.

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

20. through 24, Service providers are bound by duly executed agreements that detail their obligations for the protection, use and disclosure of personal information.

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

Reasons

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

2. Through 19, Vendor access is necessary for the system to continue to function properly.

20. Through 24, 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.

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

Halifax Water Commission

Description

1. Between January 1 and December 31, 2014, 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 sixty-four (64) times.

2. The following vendor: Tokay Navigator Software, Framingham, Massachusetts, provides initial customer data conversion and upload, periodic software maintenance and upgrades, and customer technical support.

Conditions

1. Prior to travelling, staff were advised that Halifax Water communication tools (cell phones, BlackBerrys, laptops, memory sticks, VPN) are to be used for operational requirements only and were to be password protected.

2. Vendor access is controlled through a secure network portal (no direct link to support customer account information located in SAP). Customer technical services are provided for in the annual agreement.

Reasons

1. Halifax Water staff, were approved for travelling outside Canada with their communication device(s) to ensure they remained in contact with other utility staff to fulfill operational responsibilities.

2. Vendor access is crucial to manage the Cross Connection Control Program.

Municipality of the County of Colchester

Description

Approximately six (6) staff members travelled outside Canada during calendar 2014. It is known that six (6) staff accessed personal email or stored information and email either through Outlook via a laptop or smartphone. The employees received permission from senior management.

Conditions

Employees have been notified to limit email use with smartphone'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 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

A total of three (3) employees travelled outside of the country with municipally owned devices.

Conditions

All devices 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 Richmond

Description

Three management staff travelled to the US for business. Smartphones, laptops and ipads were used while travelling.

Conditions

Access to information was done through secure network access. Each device is password protected.

Reasons

Communication between management and staff is required during travel to ensure that the ongoing day-to-day operations of municipal business are carried out.

Municipality of the District of Chester

Description

There were nine instances where four 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 (**), stay in touch regarding emergency measures issues while away (***), and to check emails on potential economic development related matters (*****).

1. To stay in touch with the office; **
2. To stay in touch with the office; ****
3. To stay in touch on operational issues and provide technical support as required; *
4. To allow for troubleshooting and IT support remotely if required; *
5. To provide IT support remotely to the Municipality; *
6. To continue to stay in touch for the purposes of REMO; ***
7. To allow troubleshooting and IT support remotely if required; *
8. To continue to stay in touch for the purposes of REMO; ***
9. To allow for troubleshooting and IT support remotely if required. *

Conditions

All devices are password protected.

Reasons

Employees were travelling for work/ and or personal reasons and require email/ access to stay connected with the Municipality's offices.

Municipality of the District of East Hants

Description

1. Constant Contact, Waltham, MA, USA, was deployed to communicate with East Hants stakeholders in 2014. Stakeholders were invited to subscribe to the service.

2. Event attendees were invited to register via Google Forms, Google Inc., Mountain View, CA, USA. They were given an option to contact the department via email.

3. Two (2) Municipal councillors travelled to the USA with their electronic devices and had access to information stored on Municipal servers within Canada. Protection of privacy protocols are followed when accessing Municipal information.

4. The Municipality of East Hants has an agreement with U.S. Bank, VISA card provider. Total Systems Services, Inc. ("TSYS"), a U.S. Bank third party service provider, stores data in the U.S. for U.S. Bank Canada commercial card clients. The data that would be stored is that which is provided by commercial card clients (name, address, telephone number, birth dates, employee numbers, etc.)

Conditions

1. Stakeholders were invited to subscribe to the email service via Constant Contact. No user data was entered without prior consent.

2. Google Form content was deleted upon retrieval of information from the form. The content was then stored on Municipality of East Hants server within Canada.

3. Access to information stored on Municipal email server via webmail and access to network via portal from the USA using mobile phones and/or laptop in the following cities: Bangor, ME; and multiple cities within New England and central USA.

4. All electronic devices are password protected, and information is accessed through the Municipal portal. All protection of privacy regulations are followed when accessing information and storing information on electronic devices. Access to personal information by foreign entities are strictly forbidden. Should an access request be received, the request must be reported to the Municipal IT Division immediately.

5. "Data at rest" for mainframe systems is stored with TSYS on encrypted Hitachi Storage Devised (HDS) and IBM Virtual Tape System (VTS) storage hardware. AES-256 encryption is enabled on all HDS and IBM hardware. Encryption used is integrated key management and no external key management is required. "Data transmitted" on mainframe systems uses Connect-Direct NDB (a third party application). U.S. Bank controls the implementation of encryption for files sent since it owns the network and router connection.

Reasons

1. The storage of information on Constant Contact and Google were necessary to conduct business in 2014 as other services were cost prohibitive. The Municipality of East Hants has explored other means of gathering personal details in 2015, including the use of Canadian server services.

2. The access of information from mobile devices and laptops were necessary to conduct Council business while visiting the USA.

3. The US Bank has been the service provider for the Municipality of East Hants for the past 15 years.

Municipality of the District of Guysborough

Description

3 employees with 2 BlackBerrys and 3 iPads.

2 employees with 2 BlackBerrys and 2 iPads

Conditions

N/A

N/A

Reasons

Business travel to stay in touch with the main office.

To keep in contact with the main office and still be able to conduct day to day business.

Municipality of the District of West Hants

Description

All critical data is housed on site at the Municipality of the District of West Hants offices. The Website data, all public data accessible from the internet is housed on a server located in Canada (iWeb, Montreal, Canada).

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. Users, from time to time, access corporate information via smartphones and tablet while travelling to other countries. All smartphones are secured with a passcode lock and the ability to remote wipe the devices should they go missing.

Reason

N/A

Municipality of the District of Yarmouth

Description

Six employees travelled outside Canada and had the ability to access personal information via one or more of the following means: cell phone, smart phone 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.

Pictou County Shared Services Authority

Description

Two employees within the Pictou County Shared Services Authority travelled outside of the country with their Pictou County Shared Services Authority owned electronic device which had been approved based on their job role within the Authority. During this time, the employees had access to the Authority's email system from their smart phone and tablet.

Conditions

Within Pictou County Shared Services Authority all smart phones and tablets have a mandatory device password provisioned. Remote access to webmail is encrypted with SSL and protected with usernames and passwords which are changed on a regular basis.

Reasons

Employees from the Pictou County Shared Services Authority may request to travel out of the country with their Pictou County Shared Service Authority provided electronic devices. A process has been put in place where the user must fill out a form and submit to the Chief Operating Officer to request permission to travel outside of the country with an Authority provided electronic device. Final decision remains with the Chief Operating Officer.

The COO will review the request from the employee and decide based on their job role with in the Pictou County Shared Services Authority if it is necessary for the user to travel with the device; such as senior staff within the Authority.

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

Six Town of Amherst staff travelled to the United States in 2014, and had access to personal information (previous emails, email addresses) via BlackBerry, iPhone or iPad; Prior approval to travel outside Canada with mobile devices was obtained from the CAO. The Town's human resource overtime, vacation and sick time information is stored within ADP EZ Labor, a product offered by ADP.

Conditions

Email access requires authentication through secure login/password. If access is required, VPN is used to access electronic data remotely. In terms of human resource information in ADP EZ Labor, authentication through secure login/password is required.

Reasons

Senior staff travelled for 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 the CAO`s approval to take any mobile devices outside Canada. In terms of our human resource services through ADP, ADP`s Global Privacy Policy requires that they protect our information and use it only for the purposes specified in our client contract with them; this assures that all ADP client data is handled in accordance with their policy, regardless of where it is processed.

Town of Annapolis Royal

Description

1. One Municipal Elected Official travelled outside Canada and had the ability to access personal information via a cell phone device. Appropriate permissions were self-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.

Conditions

1. Official is very knowledgeable and would understand that the use of communication device that can gain access to personal information should be of limited use during the time out of the country.

Reasons

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

2. The decision to allow the Town's website to go through Utah and Texas was made well before my employment with the Town of Annapolis Royal. It has been identified, and consideration will be given to moving to a host in Canada.

Town of Bridgetown[17]

Description

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

2. Website is hosted by Westcliffe Marketing (owner Andy Kerr, Hampton, NS). 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[18]

Description

Between January 1, 2014 to and including December 31, 2014, 13 staff, 2 councillors and 3 Bridgewater police officers 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, only 2 councillors accessed the Town of Bridgewater's server while out of the country. All were made aware of the requirements, etc. if they wished to access the town's server from afar and a large portion of staff had chosen to leave their devices at home and/or 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.

---

[17]Town of Bridgetown and the Town of Springhill (reported under County of Cumberland) were dissolved March 31st, 2015.

[18] Report includes Bridgewater Police Department

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 Digby

Description

One employee travelled outside of Canada on personal time and would have had access to work email via their mobile phone. This access is required in order to perform their work functions.

Conditions

Access to work email is password protected.

Reasons

Certain key employees are required to have access to work email in case of emergency work situations such as activation of our local Emergency Management Office.

Town of Lunenburg

Description

Restricted access to email on BlackBerry while travelling in USA via a secure Town of Lunenburg server with password protection and encryption. The Town also has an email spam filtering service with a company called 'GFI' that has its headquarters in the USA. This service is 'cloud based'. All email addressed to @explorelunenburg.ca first goes through the GFI server to be filtered for possible spam and is then sent to the Town's email server at the Lunenburg Town Hall. Email messages are only passed through GFI spam filter, not externally stored or accessed by it in the USA.

Conditions

As noted above.

Reasons

Required to meet operational demands when travelling with adequate security measures in place to secure all data. There is no GFI spam filter storage or access of this information outside of Canada. All information is stored and accessed on the Town's server at the Lunenburg Town Hall. Required for Town email messages to be filtered for spam messages which is accomplished through the service provided by the anti-spam filtering firm, GFI.

Town of Middleton

Description

1. All critical data is housed on site at the Town of Middleton offices.

2. The Website data, all public data accessible from the internet, is housed on a server outside Canada.

3. The Website is hosted by Westcliffe Marketing (owner Andy Kerr, Hampton, Nova Scotia, Canada). No personal information is stored or disseminated via the website. This will be moved to Canada in 2015 once the new website design is complete.

4. On occasion, municipal councillors 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. Again, all of these files are physically stored on premise 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.

5. 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[19]

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 device password provisioned and are under the control of the Town's internal BlackBerry Enterprise Server. Remote access webmail encrypted with

[19] Report includes New Glasgow Police Service

SSL and protected with usernames and passwords which are changed on 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. Process has been put place where the requesting user must out form and submit to their department head/supervisor to request permission to travel outside of the country with 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 necessary for the user to travel with the device; such senior staff or members of Council within the Municipality and senior officers within the Town's Regional Police Agency.

Town of Truro

Description

One staff member (June 2014) and one councillor (September 2014) travelled to the United States and accessed Email from cell phone.

One staff member (November 2014) travelled through the United States to Bolivia and accessed Email from cell phone.

Conditions

All were limited to email access only from centrally managed BlackBerry or iPhone device.

Reasons

The information accessed in all cases was required for business purposes of the Town of Truro.

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).

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.

Foreign Access and Storage by Municipal Police[20]

New Glasgow Police Service

Description

Employee travelled to the United States for Vacation and Work related with other police agencies.

Conditions

Agreement and approval of access to I-phone and I-pad-laptop through the Chief of Police-tech. support and Town of new Glasgow signed.

Reasons

The officer must remain in contact with the police service and management at all times.

[20] Amherst Police Department, Annapolis Royal Police Department, Cape Breton Regional Police Service, Kentville Police Service, Stellarton Police Department, Truro Police Service and Westville Police Service did not have access or storage outside of Canada to report. Bridgewater Police Department reported under the Town of Bridgewater. Cape Breton Regional Police Service reported under Cape Breton Regional Municipality. Halifax Regional Police reported under Halifax Regional Municipality. Springhill Police Department reported under the County of Cumberland.