PERSONAL INFORMATION INTERNATIONAL DISCLOSURE PROTECTION ACT

2015 Annual Report

Nova Scotia Department of Justice

Message from the Minister of Justice

I am pleased to provide the tenth 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 and respond to the concerns of Nova Scotians about the vulnerability of public sector and municipal personal information holdings to foreign access, storage and disclosure. The Act prohibits 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, 2015 to December 31st, 2015 to the Minister of Justice. This report is based on the *PIIDPA* reports received by the Policy Planning and Research 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 Act was introduced.

Original signed by

Diana Whalen

The Honourable Diana C. Whalen
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 26th, 2016 a request was sent to public bodies[1] in Nova Scotia to complete and return a *PIIDPA* Form 1 for the 2015 reporting year by March 31st, 2016. 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 2015 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 each decision made during the above-noted calendar year to allow storage or access outside Canada of personal information in the custody or under the control of the public body.

B: Restrictions or conditions placed on storage or access of the personal information outside Canada.

C: Statement of how the decisions to allow storage or access of the personal information outside Canada meet the necessary requirements of the public body's operations.

Link to previous Annual PIIDPA Reports http://novascotia.ca/just/iap/

Foreign Access and Storage by Government Departments[2]

Aboriginal Affairs

Description

1. Remote Access via electronic devices such as BlackBerrys, laptops, and tablets. There were nine (9) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email.

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.

Agriculture

Description

1. Remote access via electronic devices such as blackberries, laptops, and tablets. There were 4 instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email. V-LIMS (Veterinary Laboratory Information System) - See description of storage provided in the 2014 annual PIIDPA report.

Conditions

1. See description of conditions provided in the 2014 annual PIIDPA report. 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 sever 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; See description of reasons provided in the 2014 annual PIIDPA report

[2] Department of Business and Elections Nova Scotia did not have access or storage outside of Canada to report.

Communications Nova Scotia

Description

1. Google Analytics (GA) is the corporate standard for web analytics. Conditions or restrictions that have been placed on storage or access of personal information outside Canada include: Internet Protocol (IP) addresses will be 'marked', 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.

2. CNS is responsible for the government Twitter, Facebook, YouTube, Flickr, Tumblr, Instagram, and periscope 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.

3. Three employees of CNS travelled to the United States with BlackBerrys. Two employees also had a laptop.

Conditions

1. This information is subject to the Google Privacy Policy. (The Google Privacy Policy outlines its responsibility to protect any personal information it collects against any unauthorized access, disclosure, or destruction. It further details that they will not share any personal information without prior consent unless it is to comply with applicable laws.)

2. 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.

3. The equipment was accessed only by Communications Nova Scotia employees.

Reasons

1. Communications Nova Scotia is accountable in our business plan to report on the effectiveness of major internet (and other) campaigns. Use of Google Analytics enabled CNS to collect and report on accurate statistics about how many visitors came to government websites, from where, and approximately how long they stayed. This information allows government to refine marketing and advertising strategies ensuring that CNS provides best value to the government.

2. 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.

3. BlackBerrys were used to make calls and use email. The laptops were used to email, post messages on Facebook, access Twitter and for writing material.

Communities, Culture and Heritage[3]

Description

1. Nova Scotia Provincial Library (NSPL) maintain an integrated library system (ILS) on a cost-recovery basis for a consortium consisting of 66 brand libraries in eight regional library systems. The ILS provides a library catalogue, a purchasing module, and a circulation module (check-in/check-out, and client information).
    a. The ILS is mission critical for day to day operation of libraries. Without the ILS, libraries could not function.
    b. The ILS contain 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.
    c. The ILS is owned by an American Company, SirsiDynix, and access to personal client information from out Canada is possible with SirsiDynix and access to personal client information from outside Canada is possible with SirsiDynix. There is no Canadian vendor which supplies a similar product.

2. Continued use of Twitter and Facebook accounts. Registered Twitter Accounts include: @NS_Museum, @NS_Archives, @SailBluenoseII, @MNH_Naturalists, @NS_MMA, @FisheriesMuseum, @RossFarmMuseum, @McCullochHouse, @Highlandv, @SherbrookeNS, @0fficeofANSA @NovaScotia @GouvNE, @fundygeo @uniackeestate @ns_moi, @FFmuseumofNS @NSProvLibrary, @NS_CCH
    a. Registered Facebook Accounts include: Nova Scotia Museum, Nova Scotia Archives, Museum of Natural History, Maritime Museum, of the Atlantic, Fisheries Museum of the Atlantic, Ross Farm Museum, Sherbrooke Village Museum, Highland Village Museum, African Nova Scotian Affairs, Creative Nova Scotia, Bluenose II, Fundy Geological Museum, Museum of Industry, Le Village Historique Acadien de Ia Nouvoie-Ecosse, Perkins House Museum, Firefighters' Museum of Nova Scotia, Haliburton & Shand House Museums, lomairtean na Gäidhlig / Gaelic Affairs, Nova Scotia Provincial Library
    b. Registered Flickr Accounts include: Nova Scotia Archives, Nova Scotia Museum, Nova Scotia Provincial Library
    c. Registered Instagram Accounts include: @rossfarmmuseum, @highland_village, @firefighters_museum_ons, @fisheriesmuseum
    d. Continued use of YouTube Channels. Registered accounts are: Nova Scotia Archives, Nova Scotia Museum, Highland Village Museum, Nova Scotia Provincial Library
    e. Continued use of Pinterest and History Pin: Nova Scotia Archives

3. Ebook acess (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 storage of the personal information of libraries users on severs 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 title, to an account-based model. New users are required, and most existing users, will need to create OverDrive accounts

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

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.

4. The offering of digital access to magazines is an emerging service that many Nova Scotia public libraries have pursued on behalf of their clients this year. Nova Scotia Provincial Library manages the account with the vendor "Zinlo" on behalf of four regional public libraries.
    a. The decision to use the "Zinio for Libraries" platform was made because there was no Canadian company that is as robust as Zinio in terms of development or content.
    b. Users share their library card number, first and last name and their email address with Zinio to create their account. Other information is automatically collected based on how the user interacts with the system. Zinio's terms of use indicate that they may monitor usage to ensure compliance with terms of use.

Conditions

1. NSPL has implemented reasonable security measures to protect personal and other information in the ILS. The ILS software is maintained on a secure server in Brunswick Place.
    a. 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.
    b. NSPL enables SirsiDynix to access the server for specific upgrade activities at predetermined time periods, at the end of which SirsiDyni staff are logged out by NSPL staff.
    c. NSPL staff monitor and audit to ensure the access is reasonable and appropriate. SirsiDynix has no operational requirements to access personal information about clients.
    d. Due to these precautions, the risk of access to personal information about Nova Scotians by SirsiDynix is low, but it is technologically feasible.
    e. NSPL conducted a retroactive Privacy Impact Assessment in 2014 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. Any issues that were discovered were quickly addressed by NSPL and the appropriate regional library board.

2. N/A

3. 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 user to "opt out" of data collection metrics. This is also the ability for individuals to clear their browsing history and delete associated cookies from devices.

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

4. Zinio is a partner in the U.S. — EU Safe Harbor Framework and the U.S. — Swiss Safe Harbor Framework regarding the collection, use, and retention of personal information.
    a. Unfortunately, when we investigated further, their status on the Safe Harbour list was no longer listed as current. We have raised this with the vendor and expect that the issue will be rectified quickly.
    b. Zinio provides easy access for users to both their Privacy Policy and their Terms of Use.

Reasons

1. 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.
    a. 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.

2. 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 a cross the 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.

3. With the increased availability of technology and mobile devices, libraries are expected to provide access to digital media that is accessible to all its 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.

4. 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.

    a. 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 Zinio for libraries platform. The company serves customers worldwide from its base in the United States.

Community Services[4]

Description

1. Children in Care of the Minister of Community Services may require treatment services that are not available in the Province of Nova Scotia, and on occasion within Canada. During the 2015 calendar year, seven 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

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

information is shared with the placing facility. This information is provided to ensure that the facility will be able to meet the child's clinical needs and for the purpose of developing an appropriate treatment plan for the child. Information provided to the placing facility would include electronic information such as e-mails with agency social workers in Nova Scotia and paper copies of information identified above.

2. Six (6) staff members travelled outside of Canada with their electronic devices in 2015. Staff member travelled to Dominican Republic with iPhone from April 3-10. Staff member travelled to Florida with Blackberry and laptop from April 4-21. Staff member travelled to Jamaica with Blackberry from May 4-12. Staff member travelled to Maine with Blackberry and laptop from July 17-August 3. Staff member travelled to Georgia & North Carolina with iPhone and laptop from August 29-September 8. Staff member travelled to Maine with Blackberry and laptop from November 24 -30.

3. 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.

4. In 2015, Housing Nova Scotia made use of the free services provided by MailChimp, an e-mail marketing company located in the Georgia, United States. The service allows Housing Nova Scotia to execute e-mail campaigns to inform its stakeholders about programs, activities or any other related event. The service requires creating distribution lists, which include the names and e-mail addresses of subscribers. Every time an e-mail is sent out through MailChimp, subscribers have an opportunity to opt-out of the service. As described in the MailChimp privacy policy, the company has and may access the data on our list and the information in the e-mail. No confidential information, other than the names and e-mail addresses of subscribers, is shared through MailChimp.

5. 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 ICT Services staff within the NS Department of Internal Services. 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 Nova Scotia users. This group is also responsible for applying operating system patches and system upgrades as required.

<u>Conditions</u>

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

2. Devices were password protected.

3. 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.

4. n/a

5. 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.

Reasons

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

2. Permission was granted for staff members to travel with electronic devices for operational reasons and in order to facilitate any departmental emergency contact needs while staff were out of the country.

3. 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.

4. As part of its regular business operations, Housing Nova Scotia communicate with external stakeholders, from time to time, to inform them about the agency's activities or any related information or events it deemed important to share. MailChimp provides an efficient and cost-effective way to communicate with stakeholders via e-mail, while tracking the effectiveness of the e-mail campaign. Other than collecting names and e-mail addresses, no personal data about our subscribers is stored outside of Canada.

5. 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.

Education and Early Childhood Development

Description

1. Provincial Student Information System: The Provincial Student Information System (SIS) is used by the Nova Scotia education system (schools, school boards, Department of Education and Early Childhood Development) to manage school operations, including processes such as student registration and enrolment, attendance, student scheduling. In addition, the system is used to analyze and report on student achievement and other vital student, school, and program data for policy and program decisions.

   The SIS contains personal information regarding students and parents, including names, addresses, phone numbers, email addresses, medical, behavioural incidents, and academic records.

   This information about students and parents is necessary for the Nova Scotia education system to manage student enrollment and education from grade primary through high school.

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

3. Teacher Certification Fee Processing - The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the 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. International Programs - Transcript Payment Service: 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. Teacher Summer Professional Development Registration System: The credit card transaction information (card number, cardholder name, expiry date, CVV) is transmitted to the United States for payment authorization and reconciliation. Personal information that is transmitted through or stored outside Canada is at risk of a foreign demand for disclosure.

6. Alert Solutions – Auto-dialer software: The Alert Solutions software (auto-dialer software) was implemented in all Nova Scotia school boards.

7. Google Apps for Education: The Department of Education and Early Childhood Development uses Google Apps for Education, including services such as Drive, Gmail, Calendar, and Contacts. Users may create, store online, and share documents, presentations, spreadsheets, etc. as well domain exclusive web sites that can be shared with both internal and external users.

8. Scratch: Scratch is used by students and their teachers worldwide to program their own interactive stories, games, and animations, and share their creations with others in an online community. Scratch is a project of the MIT Media Lab and originates from the United States.

   It can be used for a range of educational purposes from science and mathematics projects, including simulations and visualizations of investigations, recordings, and interactive art and music.

   Personal information about students and teachers will be accessed and stored outside Canada as the Scratch server is located outside Canada.

9. Social Media: 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.

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

Conditions

1. Provincial Student Information System: 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 stipulates that Department of Education and Early Childhood Development staff will authorize access to the environment to the PowerSchool Group LLC, San Francisco, 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. The PowerSchool Group has no operational requirements to access personal information about clients. Therefore, the risk of access to student and parent’s personal information by the PowerSchool Group is low, but it is technologically possible.

2. TIENET: 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. Teacher Certification Fee Processing - 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. International Programs - Transcript Payment Service: 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. Teacher Summer Professional Development Registration System: 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. Alert Solutions – Auto-dialer software: 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. Google Apps for Education: Risk mitigation strategies are in place to reduce risks to personal information, including users about the risks of providing or storing personal information in a cloud service such as Google Apps for Education, establishing policies to discourage the use of these services for sensitive or confidential purposes, and use of the Google Dashboard to see what information is collected and associated with their online identity.

8. Scratch: At school, devices are subject to Internet security provided. All devices and their use are subject to the Network Access and Use Policy.

   Scratch has physical and electronic procedures to protect the information that is collected. They strictly limit individual access to the Scratch servers and the data they store on them.

9. Social Media: 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.

10. Travel with electronic devices: 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.

Reasons

1. Provincial Student Information System: The decision to contract with the PowerSchool Group for provision of the Student Information System was reached after an extensive evaluation of vendor products through a tendering process.

   The PowerSchool Group 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. TIENET: 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 Fee Processing - 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. International Programs - Transcript Payment Service: 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. Teacher Summer Professional Development Registration System: The option of payment by credit card payments is a convenience for teachers, and provides efficient and effective online services.

6. Alert Solutions – Auto-dialer software: 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. Google Apps for Education: The Department and all school boards use Google Apps for Education as a productivity tool that supports and encourages collaboration among teachers and students. This tool assists in supporting 21st century learning skills and competencies. The ubiquitous access via virtually any Internet-connected device expands opportunities for staff, teachers and students to access these resources both within and outside the school, and provides a measure of equity for all.

8. Scratch: The Department and school boards use Scratch to support the development of 21st century learning skills and competencies.

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

10. Travel with electronic devices: 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.

Energy

Description

1. Twenty-One (21) 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: UK, France, USA, Spain, Singapore, Norway, China and Australia, Staff took 65 personal and business trips outside of the country in 2015 in which they accessed government email while out of the country.

Conditions

1. 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

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

Environment

Description

1. Nine (9) employees travelled for work outside of Canada with a blackberry, cellphone, laptop, and/or tablet and may have accessed personal information. Eight (8) of the employees travelled to the United States. One (1) of the employees travelled to France.

Conditions

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

Reasons

1. When staff travel, they may be required to conduct business or maintain contact for operational purposes.

Executive Council

Description

1. Three (3) employees travelled outside of the country with their Blackberry, iPad and/or laptop devices, with the permission of the Deputy Minister. One (1) MLA travelled outside of the country with an iPad issued by the Executive Council.

Conditions

1. N/A

Reasons

1. In accordance with the Personal Information International Disclosure Protection Act (PIIDPA), an employee may be permitted to temporarily transport personal information outside of Canada if the Deputy Head considers that the transport is necessary for the performance of their duties. This include transport of personal information in a cell phone or other electronic device (e.g. a Blackberry or iPad). Also under PIIDPA, storage or access of personal information outside of Canada may be permitted by the Deputy Head if the Deputy Head considers that the storage or access is necessary to meet the requirements of the department's operation. Permission must be sought from the Deputy Head for transport and, as necessary, the storage or access of personal information while outside Canada.

Finance and Treasury Board

Description

1. Remote access via BlackBerry or other electronic devices. There were five (5) 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

1. Permission must be granted in order to take a BlackBerry or other 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 devices must be password protected.

Reasons

1. 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 blackberries, laptops, and tablets. There were four (4) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email. V-LIMS (Veterinary Laboratory Information System) - See description of storage provided in the 2014 annual PIIDPA report under Department of Agriculture.

Conditions

1. See description of conditions provided in the 2014 annual PIIDPA report. 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 sever 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. See description of reasons provided in the 2014 annual PIIDPA report.

Health and Wellness

Description

Storage

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, 2015 to December 31, 2015.

Access

The Department of Health and Wellness granted the following approval for access to personal information in the custody or control of the Department of Health and Wellness outside of Canada from January 1, 2015 to December 31, 2015:

1. **SAP Enablement for District Health Authority (DHA) Transition project**
   The Department of Health and Wellness permitted two resources from CGI Consulting, located in Germany, access to the Health SAP system. This was required to provide essential support for the SAP Enablement for DHA Transition project (SEDT). The resources were part of the CGI Global Support team and access was provisioned through a virtual private network (VPN) connection on a local Halifax desktop. Access was critical to the success of the project and limited to a period from August 18, 2015 to December 31, 2015. 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, 2015 to December 31, 2015.

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 – HealthLink811**
   In rare circumstances, Relay Health will require remote access to the information system for tier three level technical support to 811 applications. When Relay Health in the U.S. is required for this level of support, they are consulted by local 811 technical support to address related requirements and gain access to the system and associated information. 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.

5. **McKesson Corporation, Relay Health solution: Personal Health Record (PHR) Pilot Project**
   No outside of Canada system access was required or permitted in calendar year 2015.

6. **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.

7. **DHW Employee Access:**
   Between January 1, 2015 to December 31, 2015 eight (8) 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).

<u>Conditions</u>

1. **SAP Enablement for District Health Authority (DHA) Transition project**
   CGI Global team resources were limited to view only and not in possession of Nova Scotia data. Resources were required to sign non-disclosure/confidentiality agreements and access was provisioned via a virtual private network connection to a locally monitored desktop.

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

3. **McKesson Corporation, Relay Health — HealthLlnk 811**
   In 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 developers'/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 the United States' federal law which includes provisions for the protection of privacy of certain individually identifiable health information referred to as protected health information.

5. **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.

6. **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 ("HIPM") regulations and all Ministry requirements for protecting patient information in Canada. HIPAA is the United States' federal law which includes provisions for the protection of privacy of certain individually identifiable health information referred to as protected health information.

7. **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 e-mail, 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. **SAP Enablement for District Health Authority (DHA) Transition project**
   The CGI Global team resources were limited to view only and not in possession of Nova Scotia data. These resources were part of the project team who were in Germany at the time of the request. Resources were required to sign non-disclosure/confidentiality agreements and access was provisioned via a virtual private network connection to a locally monitored desktop. Access was granted to ensure that the critical path activities continued and that cost overrun was limited.

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

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

5. **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.

6. **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 heath 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.

7. **DHW Employee Access**
   When staff is traveling for business reasons (e.g. meetings, conferences), they are expected to monitor their e-mail and voicemall where possible. Therefore it is necessary for them to check e-mail 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

1. Remote access via electronic devices such as BlackBerrys, laptops, and tablets. There were nineteen (19) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email.

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.

Internal Services

Description

1. Twenty-seven (27) employees accessed their government email while travelling outside of Canada, to the United States, 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. Staff took thirty-one (31) personal and business trips outside of the country in 2015 in which they accessed government email while out of the country.

2. Pictometry Connect Explorer is a web interface that allows users to access and view photography. The system requires a username and password for access and is based in the United States. User information including first name, last name, and email address is stored in the system.

3. The OmniRim software used by the Provincial Records Centre to manage its daily operations and services was upgraded to the most recent version of the software (from version 6.0 to version 9.1). The software includes information about file retrieval requests from departmental clients who store records at the Records Centre. The upgrade was carried out by the vendor Archive Systems, Inc. based in Fairfield, New Jersey. The upgrade process included the migration of data residing on the old system to the new upgraded system. The vendor needed to have this data transferred to them on a temporary basis in order to perform the migration. This involved an initial transfer of data that the vendor analyzed in order to configure and set up the migration. After development, set up and testing was completed, there was a second transfer of data which the vendor will migrate into the upgraded system.

4. SAP Ariba provides a Cloud service to the Province (procurement services). The service includes sourcing, contract management and spend visibility. The service is hosted in the European Union.

5. 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 February 2013 to January 2016.

6. 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.

7. 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 Data centre 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 Data centre. Remote access is always controlled and monitored by CIO staff.

Conditions

1. 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.

2. Restrictions on access and location of data have been placed on the service provider. Provisions have been built into the agreement to enable a move to a Canadian data center should one be established. The vendor had indicated that the data would be securely deleted immediately after the analysis and migration phases of the project was completed. This information is subject to the Pictometry Privacy Policy

3. The vendor had indicated that the data would be securely deleted immediately after the analysis and migration phases of the project was completed.

4. SAP Ariba is governed by terms and conditions outlined in an order form for the services. The service is subject to audit to which the province is entitled to receive the audit report annually. Audit logs are also available to monitor access to PNS systems. It is not expected that any Personal Information is included in the SAP Ariba Cloud services deployed in 2015.

5. 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 with the rules of NACHA Vendors to 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.

6. 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.

7. 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 Tangoe’s offices to inspect the security measures Tangoe has in place.

Reasons

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

2. This allows the province to access oblique photographs to align with Municipal Partners. This server configuration was considered to be vulnerable and is not supported by Microsoft.

3. The OmniRim 6.0 installation which was in place needed to be upgraded to the most recent version, OmniRim 9.1, in order to address these vulnerabilities. This allowed the server side to function within the current approved network configuration, and the workstations used to access it configured as standard Windows 7 desktops. In addition, this upgrade presented us with the opportunity to improve our functionality and productivity by using an improved version which offers more streamlined work flows, better reporting, and new functions such as customer billing. The data migration (e.g., involving the transfer to the external vendor) was necessary so that the upgraded system can be used exclusively on a go-forward basis. If the migration had not taken place, the old system would have needed to be maintained for several years longer so that it could be used to access legacy data.

4. The SAP Ariba Service is not available in Canada.

5. 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.

6. 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.

7. 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[5]

Description

1. Forty (40) employees traveled outside of the country for business or personal trips with a Blackberry or laptop that contained personal information or could access personal information to the following countries: United States, Dominican Republic, Mexico, Scotland, France, China, and Cuba.

2. In 2008, JEMTEM Inc. was awarded the contract for Electronic Supervision of Offenders.

3. Automon, Legal Services Practice Manager (PM) - the vendor can access the server to do Tier II application maintenance support and to provide routine upgrade through a proxy remote access desktop session.

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.

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.

[5] Report includes the Medical Examiner’s Service and the Serious Incident Response Team (SIRT).

Conditions

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

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

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

4. The particulars about the decision, the restrictions and conditions and how this service meets the necessary requirements of Justice's operations can be found in the 2012 PIIDPA Report.

5. The particulars about the authority, the decision, the restrictions and conditions and how this meets the necessary requirements of Justice's operations can be found in the 2012 PIIDPA Report.

Reasons

1. Permission to take the electronic devices 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 the decision, the restrictions and conditions and how this service meets the necessary requirements of Justice's operations can be found in the 2012 PIIDPA Report.

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

4. The particulars about the decision, the restrictions and conditions and how this service meets the necessary requirements of Justice's operations can be found in the 2012 PIIDPA Report.

5. The particulars about the authority, the decision, the restrictions and conditions and how this meets the necessary requirements of Justice's operations can be found in the 2012 PIIDPA Report.

Labour and Advanced Education

Description

1. There were approximately seven (7) departmental employees who traveled outside Canada with a Blackberry electronic device with some contact information, for departmental operational purposes, who may have accessed personal information through email. None of the laptops, which were taken outside of Canada for departmental purposes, contained any personal information.

2. The Department of Labour and Advanced Education (LAE) utilizes NRSPro.com software for the purpose of storing and processing information, in support of the General Educational Development (GED®) program. The department scans the test sheets locally and sends data to NRSPro over an encrypted Secure Sockets Layer (SSL) connection. The information is stored in a database at NRSPro located in Spanish Fork, Utah, USA, for processing and as a record for future reference. Continued storage is required for data retrieval and combining of score results for students re-writing tests that were not passed successfully.

Conditions

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

2. The department has a contract with NRSPro which stipulates that all information will be kept private and confidential and will not be released to any third party unless authorized by the department in writing. The contract also states that only personnel authorized by the department will be provided access to store and retrieve Nova Scotia information.

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. The department completed an evaluation of options for delivery of the Nova Scotia GED® program in November of 2001. It was determined that there were only two vendors (OSS & NRSPro) certified by GEDTS to conduct test scoring that the department felt confident would be able to handle Canadian requirements. Both vendors were application service providers (ASPs) located in the USA. The ASP model included storage of the data at a vendor location in the USA. At the present time, there is no option of a software solution with data storage in Canada. SUMMARY - Sole source provider.

Municipal Affairs

Description

1. Eight (8) Department of Municipal Affairs staff travelled outside Canada during the reporting period and took their cell phone and/or laptops with them while away.

Conditions

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

Reasons

1. Allowing staff access to maintain contact with operations. Authorization to take mobile devices out of country is in accordance with the standard provincial authorization process relating to international travel and provincially provided communication devices.

Natural Resources

Description

1. Remote access via electronic devices such as blackberries, laptops, and tablets. There were ten (10) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email.

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 sever 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.

Office of the Premier

Description

1. Three (3) employees travelled outside of the country with their Blackberry and/or iPad devices, with the permission of the Chief of Staff.

Conditions

1. N/A

Reasons

1. In accordance with the Personal Information International Disclosure Protection Act (PIIDPA), an employee may be permitted to temporarily transport personal information outside of Canada if the Deputy Head considers that the transport is necessary for the performance of their duties. This include transport of personal information in a cell phone or other electronic device (e.g. a Blackberry or iPad). Also under PIIDPA, storage or access of personal information outside of Canada may be permitted by the Deputy Head if the Deputy Head considers that the storage or access is necessary to meet the requirements of the department's operation. Permission must be sought from the Deputy Head for transport and, as necessary, the storage or access of personal information while outside Canada.

Office of Immigration

Description

1. Remote access via electronic devices such as BlackBerrys, laptops, and tablets. There were eight (8) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email.

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.

Office of Planning and Priorities

Description

1. Six (6) employees travelled outside of the country with their Blackberry and/or laptop devices, with the permission of the Deputy Minister.

Conditions

1. N/A

Reasons

1. In accordance with the Personal Information International Disclosure Protection Act (PIIDPA), an employee may be permitted to temporarily transport personal information outside of Canada if the Deputy Head considers that the transport is necessary for the performance of their duties. This include transport of personal information in a cell phone or other electronic device (e.g. a Blackberry or iPad). Also under PIIDPA, storage or access of personal information outside of Canada may be permitted by the Deputy Head if the Deputy Head considers that the storage or access is necessary to meet the requirements of the department's operation. Permission must be sought from the Deputy Head for transport and, as necessary, the storage or access of personal information while outside Canada.

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 (8 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.

2. Remote access via BlackBerry or other electronic devices. On four (4) instances staff members were approved to take their BlackBerry or other electronic device while travelling outside Canada where they may have accessed personal information.

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.

2. Staff members must seek permission to take a BlackBerry or other 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 devices must be password protected.

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.

2. Staff may be required to conduct business or maintain contact with operations while traveling.

Tourism Nova Scotia

Description

1. Remote access via electronic devices such as blackberries, laptops, and tablets. There were twenty-four (24) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email.

2. Decision to continue use of Curalate. See description in 2014 Annual PIIDPA Report.

3. Decision to continue use of Mail Chimp. See description in 2013 Annual PIDDPA report.

Conditions

1. Remote access to email is protected by username/password authentication and is delivered over a secure sever link (SSL) encrypted link. All government issued electronic devices must be password protected.

2. Mail Chimp, see conditions in 2013 Annual PIDDPA report.

3. Curalate, see conditions provided in the 2014 annual PIIDPA report. Permission must be granted in order to take an electronic device out of the country.

Reasons

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

2. Curalate, see description of reasons provided in the 2014 annual PIIDPA report.

3. MailChimp -see description of reasons provided in the 2013 annual PIIDPA report.

Transportation and Infrastructure Renewal

Description

1. There were thirty-six (36) employees who were approved to access their wireless devices (e.g., cell phones/BlackBerrys/iPhones/iPads/laptops) while travelling outside Canada for business and pleasure in 2015. Two (2) travelled to Europe during the period of March - May 2015, one (1) to Turks & Caicos during period of April 2015 and thirty-three (33) to United States during the period of February - December 2015. Blackberries and other electronic devices utilized by staff while 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, were approved to take government end-user devices with them when there were no other staff with equivalent skills to sustain service delivery in his/her area during their absence.

2. 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. 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. Employees are expected to maintain communication with staff at the office and ensure that their wireless devices are password protected and that the Government server is utilized.

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

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

Reasons

1. Permission to take wireless devices outside the country was granted to all employees to maintain contact with their staff to deal with urgent matters while travelling and to meet the requirements of the department's operations.

2. Promotion of road safety and law enforcement so that a driver's license or vehicle permit may not be fraudulently transferred from one jurisdiction to another and infractions occurring in another jurisdiction are recorded on the driver's record in Nova Scotia.

3. This agreement has been in place since 1999 with security measures in place since then. In FY 13/14, it was confirmed that only IRP jurisdictional staff have access to this information which is password protected on a secure web site.

Service Nova Scotia[6]

Description

1. Five (5) Service Nova Scotia (SNS) staff traveled outside Canada during the reporting period on five (5) separate occasions and took their laptop and/or Smart phone while away.

2. SNS currently stores approximately 19,864 boxes of records with Iron Mountain.

3. Credit card transaction information resulting from payments for online services under the ACOL Contract or the 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.

4. In 2006, MorphoTrust USA (formerly L-1 Identity Solutions) (formerly Digimarc) of Billerica, Massachusetts was awarded the 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 usage/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 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.

5. 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.

[6] Report includes Alcohol, Gaming, Fuel and Tobacco Division.

Conditions

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

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

3. All service providers in the credit card payment claim 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.

4. Access from the Billerica and Fort Wayne locations is restricted via VPN username/password and on the image/database server by the privileged account username/password. Access will be in response to escalated support calls only.

5. 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.

Reasons

1. Maintain contact with operations.

2. The Provincial Records Centre used to store their records overflow at Iron Mountain in the late to mid 1990s. In 1997, the Iron Mountain accounts created by the Provincial Records Centre were transferred to the various departments who had overflow records stored with Iron Mountain. At this time, SNSMR, now 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 STOR had 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 to space restrictions within their operating offices.

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

4. 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.

5. 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.

Foreign Access and Storage by Agencies, Boards & Commissions and Other Public Bodies[7]

Halifax Harbour Bridges[8]

Description

1. HHB's MACPASS software application maintenance and support is provided by BRiC (previously 3M) primarily located in Irvine, California. BRiC provides both routine maintenance and upgrade and have access to personal information through a virtual private network into HHB's internal network. Access is fairly routine and would occur minimally once a month.

2. HHB utilizes BoardBookit (headquartered in Pittsburgh, Pennsylvania); a secure board portal solution to provide secure, intuitive and powerful tools to enhance information sharing, communication and improve governance for board members. Information stored on BoardBookit contains minimal personally identifiable information.

3. HHB requires written permission authorized by the CEO to take devices outside of the country. All electronic devices (iPads, iPhones) are password protected and email is delivered over a secure server (SSL) encrypted link. All laptops are protected with a username and password and employees requiring access to HHB's network connect over a virtual private network that uses dual layer authentication (domain authentication and a token).

4. Use of Social Media: HHB's communications department manages two twitter accounts. One account, @HHBridges, is used to share information about the status of the bridges in terms of traffic. It is linked to the provincial 511 system and is updated every hour (more often if there is an issue that needs to be communicated).

   HHB also uses the account to share photos and short videos and other communications it wants to share with the public. The public use Twitter to communicate directly with as well with their questions and comments.

   The second account is @BigLiftHFX and is used to communicate the status of the Big Lift Project.

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

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

[7] Council on African-Canadian Education, Human Rights Commission, Nova Scotia Health Research Foundation, Nova Scotia Liquor Corporation (NSLC), Nova Scotia Provincial Lotteries and Casino Corporation, Nova Scotia Public Service LTD Plan, Office of the Police Complaints Commissioner, Resource Recovery Fund Board Nova Scotia (RRFB Nova Scotia), and Workers' Compensation Appeals Tribunal did not have access or storage outside of Canada to report.

[8] Formerly operated as Halifax-Dartmouth Bridge Commission

Other social media sites HHB uses includes: Facebook, Instagram, and YouTube. We don't collect any personal information on these sites.

Conditions

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

2. All traffic is over secure https protocol using high strength encryption certificates, highly secure Tier 1 hosting, redundant managed firewalls with VPN and PCI Compliant, SSAE-16 compliant (formerly SAS70), full-strength encryption and central administrative control (web and mobile). All web data transmitted to/from BoardBookit application is TLS/SSL encrypted. Permissions and access within BoardBookit are tied to individual users administered by HHB.

Reasons

1. The MACPASS back office software application is a propriety software application which is critical to HHB and its ability to conduct and operate its electronic toll collection system.

2. Limited availability for a cost effective service in Canada.

3. Staff may be required to conduct business or maintain contact with operations when travelling out of the country. There were a total of six (6) occurrences (of four (4) different employees) travelling with their laptop or other electronic devices as noted below:

   - October 2015- Wyoming, Wyoming, USA;
   - November 2015 – New York (2 employees);
   - March 2016 – British Virgin Islands;
   - February 2016 – Jamaica and Washington, DC;
   - March 2016 – Mexico.

Innovacorp

Description

1. DealFlow - Sevanta Systems provides software and workflow consulting services to venture firms, private equity groups, and Fortune 500 corporate investment teams throughout the world. Launched in 2005, Sevanta Dealflow, was designed as a full-service, customizable dealflow management solution. Sevanta Systems Corporation is a U.S. corporation headquartered in Miami, Florida. Pursuant to s. 5(2) PIIDPA Innovacorp's president and CEO determined the storage/access outside Canada of business information in Innovacorp's custody/control, as part of the investment relationship management data services supplied under contract by mydealflow.com are to meet the necessary requirements of Innovacorp's operation.

2. SurveyMonkey - An online survey development cloud-based software-as-a-service company, founded in 1999. SurveyMonkey provides free, customizable surveys, as well as a suite of paid back-end programs that include data analysis, sample selection, bias elimination, and data representation tools, storage and access of anonymous employee survey data. Pursuant to s. 5(2) PIIDPA Innovacorp's president and CEO determined the storage/access outside Canada of

anonymous employee survey data as part of the management of the employment relationship. This corporation with its principal place of business in San Francisco, California, is to meet the necessary requirements of Innovacorp's operation.

3. Innovacorp Client Engagement and Communications is responsible for Innovacorp’s Twitter, Facebook, Instagram and YouTube accounts, which are based in the U.S. These accounts are used for sharing Innovacorp news releases, videos, photos and other information to a broader audience.

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

Conditions

1. Dealflow - Sevanta Systems provides software and workflow consulting services to venture firms, private equity groups, and Fortune 500 corporate investment teams throughout the world. Launched in 2005, Sevanta Dealflow, was designed as a full-service, customizable dealflow management solution. Data services includes storage and access of client/partner representatives' personal information (primarily business information). The individuals' business information is to be protected in accordance with the company’s master agreement and privacy statement which recognize Innovacorp as owner of the stored data and provide strong privacy protection and security processes. The service uses a 256-bit, bank-grade certificate to encrypt the connection between browser and Sevanta’s servers.

2. SurveyMonkey - An online survey development cloud-based software as a service company, founded in 1999. SurveyMonkey provides free, customizable surveys, as well as a suite of paid back-end programs that include data analysis, sample selection, bias elimination, and data representation tools, email campaign management services - storage and access of anonymous employee survey data is to be protected in accordance with the SurveyMonkey terms of service.

3. Innovacorp uses social media platforms to share information and create public, client and potential client engagement. Innovacorp retweets other partner accounts and public information from partners (Volta, MaRS, Province of NS, etc.).

4. Innovacorp 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 Innovacorp 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 Innovacorp’s code of conduct and Innovacorp information technology policy.

Reasons

1. Dealflow - client/partner information, primarily business information - Innovacorp requires a robust and secure platform to store and manage information necessary for the conduct of Innovacorp's investment relationships with its clients, prospective clients, partners and stakeholders. The Dealflow data service was selected through independent evaluation and based on its 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 information (given its more accessible public nature) being the target of a foreign demand for disclosure.

2. SurveyMonkey - An online survey development cloud-based software-as-a-service company, founded in 1999. SurveyMonkey provides free, customizable surveys, as well as a suite of paid back-end programs that include data analysis, sample selection, bias elimination, and data representation tools - storage and access of anonymous employee survey data. Domestic suppliers currently do not meet Innovacorp's technical and service requirements.

3. Social media platforms are used to increase public awareness and engagement, and share information with client and potential clients.

4. Innovacorp’s directors, officers, employees performance of duties during international travel - storage and access - personal information - For business continuity purposes, Innovacorp 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 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. -e-mail campaign management services -storage and access -individuals' business contact information (primarily e-mail addresses) Pursuant to s. 5(2) PIIDPA the head of Nova Scotia Business Inc. (NSBI) determined the storage / access outside Canada of individuals' business contact information (primarily e-mail addresses) in NSBI's custody / control, as part of e-mail campaign management services supplied under contract by VerticalResponse, Inc. (a US corporation with its principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.

3. TinderBox Inc. -sales proposal management services -storage and access -prospective client representative's business contact information (name, e-mail address) and proposal interaction analytics (to March 31, 2015) Pursuant to s. 5(2) PIIDPA the head of Nova Scotia Business Inc. (NSBI) determined the storage / access outside Canada of individuals' business contact information (name, e-mail addresses) and proposal interaction analytics information in NSBI's custody / control, as part of the sales proposal management services supplied under contract by TinderBox Inc. (a US corporation based out of Indianapolis, Indiana) is to meet the necessary requirements of NSBI's operation.

4. Proposify (PitchPerfect Software, Inc.) -sales proposal management services -storage and access -prospective client representative's business contact information (name, e-mail address) and

proposal interaction analytics (after March 31, 2015) Pursuant to s. 5(2) PIIDPA the head of Nova Scotia Business Inc. (NSBI) determined the storage / access outside Canada of individuals' business contact information (name, e-mail addresses) and proposal interaction analytics information in NSBI's custody / control, as part of the sales proposal management services supplied under contract by Proposify (PitchPerfect Software, Inc.) a Canadian company operating from Dartmouth, Nova Scotia with servers in Reston, North Virginia, is to meet the necessary requirements of NSBI's operation.

5. 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.;

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

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

3. TinderBox Inc. -sales proposal management services -storage and access -prospective client representative's business contact information (name, e-mail address) and proposal interaction analytics (to March 31, 2015) The individuals' business contact information (name, e-mail 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. Proposify (PitchPerfect Software, Inc.) -sales proposal management services -storage and access -prospective client representative's business contact information (name, e-mail address) and proposal interaction analytics (after March 31, 2015) The individuals' business contact information (name, e-mail address) and proposal interaction analytics is to be protected in accordance with the Proposify service agreement, privacy policy and security statement which recognize NSBI as owner

of the stored data and confirms privacy protection and the implementation of commercially reasonable security measures.

5. 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.

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

3. TinderBox Inc. -sales proposal management services -storage and access -prospective client representative's business contact information (name, e-mail address) and proposal interaction analytics (to March 31, 2015) 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. Proposify (PitchPerfect Software, Inc.) -sales proposal management services -storage and access -prospective client representative's business contact information (name, e-mail address) and proposal interaction analytics (after March 31, 2015) 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.

5. 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.

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

Nova Scotia Legal Aid Commission

Description

1. 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.

Conditions

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

Reasons

1. 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 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 was one instance where two (2) employees traveled outside of Canada with the ability to access personal information through a secure portal into the Board's internal network via mobile device or remote access.

Conditions

1. Off-site storage provided by foreign entity subsidiary: Payroll Service. The service provider has agreed not to store information outside of Canada.

2. Employee Access to Personal Information by Mobile Device. Employee Access to Personal Information by Mobile Device (Blackberry or Computer). Access to the Board's internal network is

protected by username/password authentication and is delivered over a secure portal. Employees are required to use this portal when accessing personal information. Employees are also required to immediately report any theft or loss of the device or any suspected breach of information.

Reasons

1. Off-site storage provided by foreign entity subsidiary: Payroll Service. No suitable compliant service provider has been found in Canada.

2. Employee Access to Personal Information by Mobile Device. Employee Access to Personal Information by Mobile Device (Blackberry or Computer). When traveling staff may be expected to monitor their email and voicemail for business continuity and to fulfill their job related responsibilities.

Securities Commission

Description

1. Remote Access via Blackberry or other electronic device – There were twenty-eight (28) instances where staff members were approved to take their Blackberry or other electronic device while travelling outside Canada and may have accessed personal information.

Conditions

1. See description of restrictions or conditions placed on access (or storage) provided in the 2014 annual PIIDPA report.

Reasons

1. See description of reasons to allow access (or storage) provided in the 2014 annual PIIDPA report.

Trade Centre Ltd.

Description

1. 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

1. Only Ticket Atlantic employees and agents can access the information through the secured VPN tunnel. Our contract states that Paciolan will only use the collected customer information 'solely for the purposes contemplated in this agreement and otherwise in compliance with all applicable federal and state laws. The customer will own all personal information, data and related information collected or received through use of the system by it, or directly by Paciolan, and all compilations thereof, in connection with the operation of the system. Data is stored to ensure we can reconcile

delivery of tickets, returns, discrepancies and payment verification to the customer. Only customers who have given prior permission or who have subscribed to Ticket Atlantic's Insiders Club will 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

1. 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 the contract was found to be sound.

Waterfront Development

Description

1. 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.

2. Facebook/Twitter/Youtube/Instagram

3. Google Analytics is used to monitor website traffic.

4. Dropbox- online file storage tool.

5. Basecamp – project management tool.

6. GTechna – online permit management system, parking and traffic enforcement software.

7. Sentinel is an on-line tool used to access parking data which includes machine operation notifications, transactions, revenue collection and maintenance information.

Conditions

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

2. No IP addresses or personal information is collected 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. Google Analytics is a service provided by Google, based in the US. Google Analytics records the IP addresses 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.

4. Dropbox is located in the US.

5. Basecamp is located in the US.

6. GTechna is a company based in St. Laurent, Quebec; however, the server is located in Atlanta, Georgia. No banking or credit card information is processed through this system.

7. Sentinel is stored with Core Network Solutions and the servers are located in Grand Rapids, Michigan.

Reasons

1. When staff travel for business, they are required to be available by phone and monitor their email and voicemail for business continuity and operational purposes.

2. All social media is based in the United States. These accounts are used for sharing news releases, videos, photos and other information to a broader audience.

3. Analytical information allows Waterfront Development to monitor use of the website and for purposes of developing marketing strategy and evaluation.

4. Dropbox is used to allow individuals access to larger files via protected password.

5. Basecamp is used to allow management, operations and maintenance staff to be on top of all current projects on the go.

6. Waterfront Development updated the parking enforcement system in June 2015. JJ MacKay, a Nova Scotia based company that provides the parking hardware and machinery, recommended the online system through GTechna.

7. Waterfront Development updated the Halifax Waterfront parking system in June 2015 with JJ MacKay, the only Canadian supplier of parking infrastructure. Sentinel is JJ MacKay’s back-end data centre that allows clients to access information related to their parking system.

Workers’ Compensation Board of Nova Scotia

Description

1. Employee access to personal information by mobile device (iPhone, iPad, Blackberry) or computer (laptop, desktop): 63 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: 311 individual's personal information (contained in unique claim files) accessed from a remote location outside of Canada (e.g., in the US) through a secure portal into the WCB's internal network by remote access.

3. Medical Consultant access to personal information: 55 instances of access to personal information (contained in unique claim files) accessed from a remote location outside of Canada (e.g., in the US) through a secure portal into the WCB's internal network by remote access.

4. Translation Services: 12 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 based on accepted industry practices. 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 based on accepted industry practices. 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 based on accepted industry practices. 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), or 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 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.

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[9]

Nova Scotia Health Authority

Description

1. Vendors requiring access to personal information from outside of Canada are granted access on a need to know basis as necessary for the operations of the health authority, or when the expertise does not exist in house, or is not available in Canada. We have agreements and contracts with multiple vendors and NSHA IT facilitates access as needed. Some examples of Vendors and locations are as follows: Medstation (Pharmacy), San Diego, California, US; Mayo Collaborative Services , Inc (Mayo Laboratories) in MN, US; ORAU Oak Ridge Associated Universities (Laboratory Testing) in TN, US; Haemonetics (Laboratory Testing), United States; 16s DNA Sequencing is sent to McLab in San Francisco, California, US; Krankenhaus Mara GmbH (laboratory Testing) in Bethel, Germany; Remetco (x-ray film removal company), US; Chestnut Health Systems (Mental Health and Addiction Certification Company), US; Omnicell (Pharmacy Dispensing Equipment), US; e-Scription/Nuance (Medical Dictation), US; Medtronic (Pacemakers), US.

2. Staff members reported 48 instances of travelling outside of Canada and may have accessed personal information or company e-mail via remote access or their Blackberry. Personal Health Information (PHI) is not typically accessed while staff members are travelling outside of the country.

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. Each former district'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 each former district's Remote Access Policy. Employees must receive approval to bring their NSHA issued electronic devices out of the country.

Reasons

1. Current access to and storage of information outside of Canada is tied to NSHA programs and/or systems that are necessary for operations. When Privacy Impact Assessments are reviewed for new or upgraded technology special attention is paid to ensure that PIIDPA is complied with.

2. Staff members may be granted approval to access PHI when travelling for the following purposes: patient care, business continuity, and operational support.

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

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 2015 calendar year, IWK worked with 85 American laboratories, 48 international and 49 Canadian laboratories. All labs are reviewed for quality guidelines twice a year. It should be noted that not all labs are used on an annual basis.

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 Nova Scotia Internal Services Department 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:
    a. Meditech: Boston, Massachusetts, USA (IWK patient information system);
    b. Agfa: Wilmington, Massachusetts, USA (medical imaging equipment and supplies); Pyxis: San Diego, California, USA (medical safety systems and technology);
    c. EMC Corporation: Hopkinton, Massachusetts, USA (healthcare data and information sharing services and technology);
    d. Blackbaud: Charleston. South Carolina, USA (non-profit management/accounting software);
    e. Draeger Medical - Innovian system : Germany and USA (IWK anesthesia system);
    f. Genial Genetics: United Kingdom (laboratory software for genetic data management);
    g. Innovian: Germany and USA (IWK anesthesia system);
    h. Masimo Corporation: Irvine. California USA (support for clinical monitors in Medical Surgical and Neuroscience Unit and Pediatric Medical Unit);
    i. Alere Infomatics: Tampa, Florida, USA (support for glucose meter management system);
    j. Forward Advantage (Meditech – faxing) – California, USA
    k. GE Healthcare: United Kingdom (ultrasound system); and USA
    l. Perklin Elmer: Akron Ohio USA (Newborn Screening Program/SpecimenGate application)
    m. Phillips (Obstertical Trace View , Ecelera system Cardiology)

3. Business Travel: IWK's records indicate that during the 2015 calendar year, there were approximately 84 incidents of travel booked through the IWK for work-related travel outside of Canada, by 77 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 e-mail and/or telephone access while staff are traveling internationally,

Conditions

1. Restrictions or Conditions: 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 e-mail 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:

    a. "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.

    b. IWK blackberries 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.

c. IWK laptops use encryption software to safeguard information stored on any lost, stolen or improperly accessed 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

Foreign Access and Storage by Universities and Colleges[10],

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 US, data on university alumni and donors is housed on servers at the CBU campus. Blackbaud does provide remote technical service. If authorized by the university, it is possible for a Blackbaud technician to access the CBU system under CBU supervision.

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

3. Course Management System: CBU uses MOODLE as its course management system. The system facilitates on-line learning for both on-campus students and those studying from a distance. Web access is available to this system for both faculty delivering courses and students enrolled in the courses.

4. Residence Management: CBU utilizes StarRez, a Residence Management System provided through StarRez Inc. from Greenwood Village, 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.

8. HubSpot: HubSpot is an inbound marketing and sales software platform used by the CBU Marketing and Communications Department. Hubspot has offices Cambridge Mass. Doublin 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

[10] Acadia University and Atlantic School of Theology did not have access or storage outside of Canada to report.

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 approximately 45 international trips to 17 different countries in 2015. 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

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. 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 e-mail 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

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. 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[11]

Description

1. Web-Based RCT Platform: Web-Based randomized controlled trial platform to conduct sleep intervention research. (Storage in United States)

2. Online Exam Preparation: See description of storage provided in the 2014 annual PIIDPA report.

[11] Report includes the Nova Scotia Agricultural College

3. Event Registration Management Tool: See description of storage provided in the 2014 annual PIIDPA report.

4. Online Communications and Collaboration Tools: See description of storage provided in the 2013 annual PIIDPA report.

5. Athletics Schedules and Scores: See description of storage provided in the 2013 annual PIIDPA report.

6. Academic Instructional Tools: See description of storage provided in the 2013 annual PIIDPA report.

7. College Student Inventory (CSI): See description of storage provided in the 2013 annual PIIDPA report.

8. Financial Services Electronic Forms: See description of access provided in the 2012 annual PIIDPA report.

9. University ID Card: See description of access provided in the 2012 annual PIIDPA report.

10. Network and Systems Upgrades: See description of access provided in the 2012 annual PIIDPA report.

11. Wireless Products: See description of storage provided in the 2012 annual PIIDPA report.

12. Apple Warranty Maintenance: See description of storage provided in the 2012 annual PIIDPA report.

13. Teaching and Research Statistical Software: See description of access provided in the 2012 annual PIIDPA report.

14. Collaborative Teaching Software: See description of access provided in the 2012 annual PIIDPA report.

15. Service Provider Maintenance (IBM Hardware and Software): See description of access provided in the 2012 annual PIIDPA report.

16. Administrative Computing Software: See description of access provided in the 2012 annual PIIDPA report.

17. Room Reservations Software: See description of access provided in the 2012 annual PIIDPA report.

18. Degree Progress Software: See description of access provided in the 2012 annual PIIDPA report.

19. Student Advising Scheduling Software: See description of access provided in the 2012 annual PIIDPA report.

20. Student Performance and Referral Software: See description of access provided in the 2012 annual PIIDPA report.

21. Medical Education Evaluations Software: See description of access provided in the 2012 annual PIIDPA report.

22. Dentistry Academic Materials Software: See description of storage provided in the 2012 annual PIIDPA report.

23. Service Provider Maintenance (Xerox Hardware and Software): See description of access provided in the 2012 annual PIIDPA report.

24. Website Feedback: See description of storage provided in the 2012 annual PIIDPA report.

25. Plagiarism Detection: See description of storage provided in the 2012 annual PIIDPA report.

26. Law Student Survey: See description of storage provided in the 2012 annual PIIDPA report.

27. Undergraduate Student Survey: See description of storage provided in the 2012 annual PIIDPA report.

28. Hosted Learning Management System: See description of access provided in the 2012 annual PIIDPA report.

29. Student Learning Outcomes Software: See description of access provided in the 2012 annual PIIDPA report.

30. Environmental Health & Safety Database: See description of access provided in the 2012 annual PIIDPA report.

31. Online Law School Exams: See description of access provided in the 2012 annual PIIDPA report.

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

Conditions

1. Web-Based RCT Platform. 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. Service provider privacy policy. Technical security measures are in place to protect the data, including encryption.

2. Online Exam Preparation. See description of storage provided in the 2014 annual PIIDPA report.

3. Event Registration Management Tool. See description of storage provided in the 2014 annual PIIDPA report.

4. Online Communications and Collaboration Tools. See description of storage provided in the 2013 annual PIIDPA report.

5. Athletics Schedules and Scores. See description of storage provided in the 2013 annual PIIDPA report.

6. Academic Instructional Tools. See description of storage provided in the 2013 annual PIIDPA report.

7. College Student Inventory (CSI). See description of storage provided in the 2013 annual PIIDPA report.

8. Financial Services Electronic Forms. See description of access provided in the 2012 annual PIIDPA report.

9. University ID Card. See description of access provided in the 2012 annual PIIDPA report.

10. Network and Systems Upgrades. See description of access provided in the 2012 annual PIIDPA report.

11. Wireless Products. See description of storage provided in the 2012 annual PIIDPA report.

12. Apple Warranty Maintenance. See description of storage provided in the 2012 annual PIIDPA report.

13. Teaching and Research Statistical Software. See description of access provided in the 2012 annual PIIDPA report.

14. Collaborative Teaching Software: See description of access provided in the 2012 annual PIIDPA report.

15. Service Provider Maintenance (IBM Hardware and Software). See description of access provided in the 2012 annual PIIDPA report.

16. Administrative Computing Software. See description of access provided in the 2012 annual PIIDPA report.

17. Room Reservations Software. See description of access provided in the 2012 annual PIIDPA report.

18. Degree Progress Software. See description of access provided in the 2012 annual PIIDPA report.

19. Student Advising Scheduling Software. See description of access provided in the 2012 annual PIIDPA report.

20. Student Performance and Referral Software. See description of access provided in the 2012 annual PIIDPA report.

21. Medical Education Evaluations Software. See description of access provided in the 2012 annual PIIDPA report.

22. Dentistry Academic Materials Software. See description of storage provided in the 2012 annual PIIDPA report.

23. Service Provider Maintenance (Xerox Hardware and Software). See description of access provided in the 2012 annual PIIDPA report.

24. Website Feedback. See description of storage provided in the 2012 annual PIIDPA report.

25. Plagiarism Detection. See description of storage provided in the 2012 annual PIIDPA report.

26. Law Student Survey. See description of storage provided in the 2012 annual PIIDPA report.

27. Undergraduate Student Survey. See description of storage provided in the 2012 annual PIIDPA report.

28. Hosted Learning Management System. See description of access provided in the 2012 annual PIIDPA report.

29. Student Learning Outcomes Software. See description of access provided in the 2012 annual PIIDPA report.

30. Environmental Health & Safety Database. See description of access provided in the 2012 annual PIIDPA report.

31. Online Law School Exams. See description of access provided in the 2012 annual PIIDPA report.

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

Reasons

1. Web-Based RCT Platform. Essential to ongoing research project. No viable Canadian alternatives in terms of experience, functionality and customization.

2. Online Exam Preparation. See description of storage provided in the 2014 annual PIIDPA report.

3. Event Registration Management Tool. See description of storage provided in the 2014 annual PIIDPA report.

4. Online Communications and Collaboration Tools. See description of storage provided in the 2013 annual PIIDPA report.

5. Athletics Schedules and Scores. See description of storage provided in the 2013 annual PIIDPA report.

6. Academic Instructional Tools. See description of storage provided in the 2013 annual PIIDPA report.

7. College Student Inventory (CSI). See description of storage provided in the 2013 annual PIIDPA report.

8. Financial Services Electronic Forms. See description of access provided in the 2012 annual PIIDPA report.

9. University ID Card. See description of access provided in the 2012 annual PIIDPA report.

10. Network and Systems Upgrades. See description of access provided in the 2012 annual PIIDPA report.

11. Wireless Products. See description of storage provided in the 2012 annual PIIDPA report.

12. Apple Warranty Maintenance. See description of storage provided in the 2012 annual PIIDPA report.

13. Teaching and Research Statistical Software. See description of access provided in the 2012 annual PIIDPA report.

14. Collaborative Teaching Software: See description of access provided in the 2012 annual PIIDPA report.

15. Service Provider Maintenance (IBM Hardware and Software). See description of access provided in the 2012 annual PIIDPA report.

16. Administrative Computing Software. See description of access provided in the 2012 annual PIIDPA report.

17. Room Reservations Software. See description of access provided in the 2012 annual PIIDPA report.

18. Degree Progress Software. See description of access provided in the 2012 annual PIIDPA report.

19. Student Advising Scheduling Software. See description of access provided in the 2012 annual PIIDPA report.

20. Student Performance and Referral Software. See description of access provided in the 2012 annual PIIDPA report.

21. Medical Education Evaluations Software. See description of access provided in the 2012 annual PIIDPA report.

22. Dentistry Academic Materials Software. See description of storage provided in the 2012 annual PIIDPA report.

23. Service Provider Maintenance (Xerox Hardware and Software). See description of access provided in the 2012 annual PIIDPA report.

24. Website Feedback. See description of storage provided in the 2012 annual PIIDPA report.

25. Plagiarism Detection. See description of storage provided in the 2012 annual PIIDPA report.

26. Law Student Survey. See description of storage provided in the 2012 annual PIIDPA report.

27. Undergraduate Student Survey. See description of storage provided in the 2012 annual PIIDPA report.

28. Hosted Learning Management System. See description of access provided in the 2012 annual PIIDPA report.

29. Student Learning Outcomes Software. See description of access provided in the 2012 annual PIIDPA report.

30. Environmental Health & Safety Database. See description of access provided in the 2012 annual PIIDPA report.

31. Online Law School Exams. See description of access provided in the 2012 annual PIIDPA report.

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

Mount Saint Vincent University

Description

1. 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

1. 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

1. 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 databases containing personal data are stored in Canada and are carefully monitored. Access to this data from outside Canada is permitted in the following cases:

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

2. Trained vendor technicians from the U.S. are permitted access when providing support for University systems.

3. Employees of NSCAD University use Microsoft Office 365 for e-mail, storage and collaboration. As some of the Microsoft servers may reside outside of Canada, it is possible for personal information to inadvertently be stored on those servers.

Conditions

NSCAD University places the following conditions and restrictions on personal information 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 session must be authorized by the Director, Computer Services, and attended by an employee authorized by the Director, Computer Services.

3. In the case of Office 365, we provide training and documentation to promote the use of Office 365 as a secure, industry-standard solution. We provide information on the protection of privacy and encourage employees to avoid storing or communicating private information unless it is necessary to the performance of their job.

Reasons

1. Providing authorized access to our Enterprise data while employees are travelling allows them to service International students across time zones and prevents the use of less secure forms of information, such as e-mail, local computer files or paper-based data.

2. Expert support for our enterprise systems is only available from the vendor. NSCAD uses industry standard method in this regard.

3. Cloud based e-mail, storage and collaboration software is now industry-standard. NSCAD works in collaboration with several other Universities in Nova Scotia in this regard.

Nova Scotia Community College

Description

1. As required by section 5(3) of the Personal Information International Disclosure Protection Act (PIIDPA) the Nova Scotia Community College is reporting that it has allowed for the storage of personal information under our control to be stored on servers located outside of Canada. The College committed to the move to Office 365 during 2015. Office 365 will see our user accounts registered on Microsoft's servers that are located outside Canada and users will be able to store and access data outside Canada. Office 365 includes Exchange Online Protection, which is an antivirus protection mechanism. The Higher Education Information Technology Shared Services Group is funded by the Province of Nova Scotia and is facilitating the move of all post-secondary

educational institutions in the province to move to Office 365. Microsoft is currently exploring options to open up a Canadian data centre in 2016.

2. As required by the Act, I would also like to inform you that:

   - The College will allow our employees to transport personal information temporarily outside Canada but only to the extent that it is strictly necessary for their assigned duties or as a necessary part of a research project. We anticipate that this information will be transported using cellular telephones, wireless handhelds, laptops and storage devices. In such event, employees will be required to take all reasonable precautions (e.g. encryption) to protect the personal information.

   - For accessing personal information in College data repositories from outside Canada; the College will permit its employees and students to use web-based or other internet access tools if it is a necessary part of performing his or her assigned duties or as a necessary part of a research project.

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

Conditions

See Description above

Reasons

See Description above

St. Francis Xavier

Description

1. Bi-Tech: See description of access and/or storage provided in the 2014 annual PIIDPA report.

2. Kinetics Software: See description of access and/or storage provided in the 2014 annual PIIDPA report.

3. EZ Facility: See description of access and/or storage provided in the 2014 annual PIIDPA report.

4. StFX.ca Website: See description of access and/or storage provided in the 2014 annual PIIDPA report.

5. Salesforce.com: See description of access and/or storage provided in the 2014 annual PIIDPA report.

6. St. FX offers an optional notification service by utilizing the mass notification software provided by Everbridge of Glendale CA to provide campus updates to students, faculty and staff. Personal information is limited to a name and chosen contact information. StFX data is stored in Canada.

7. WC Online is a student appointment booking/scheduling software used by several departments of the University. The product is provided by Twenty Six Design, based out of Celebration FL. StFX data is stored in Canada.

8. StFX has a site license for a survey tool provided by Fluid Survey, who were acquired by Survey Monkey, head quartered in Palo Alto, CA with Offices in Ottawa. StFX Data is stored in Canada.

Conditions

1. See description of access and/or storage provided in the 2014 annual PIIDPA report.

2. See description of access and/or storage provided in the 2014 annual PIIDPA report.

3. See description of access and/or storage provided in the 2014 annual PIIDPA report.

4. See description of access and/or storage provided in the 2014 annual PIIDPA report..

5. See description of access and/or storage provided in the 2014 annual PIIDPA report.

6. Access to Everbridge data outside of Canada are limited to StFX users who may be out of the country but need to access information. Information is protected and limited to authorized users through industry standard data security, encryption and authentication practices.

7. Access to WC Online above outside of Canada are limited to StFX users who may be out of the country but need to access information. Information is protected and limited to authorized users through industry standard data security, encryption and authentication practices.

8. Access to the Fluid Survey data outside of Canada are limited to StFX users who may be out of the country but need to access information. Information is protected and limited to authorized users through industry standard data security, encryption and authentication practices.

Reasons

1. See description of access and/or storage provided in the 2014 annual PIIDPA report.

2. See description of access and/or storage provided in the 2014 annual PIIDPA report.

3. See description of access and/or storage provided in the 2014 annual PIIDPA report..

4. See description of access and/or storage provided in the 2014 annual PIIDPA report.

5. See description of access and/or storage provided in the 2014 annual PIIDPA report.

6. Everbridge was chosen for best meeting operational needs, functionality, data security and cost as compared to known alternatives.

7. WC Online was chosen for best meeting operational needs, functionality, data security and cost as compared to known alternatives.

8. Fluid Survey was chosen for best meeting operational needs, functionality, data security and cost as compared to known alternatives.

St. Mary’s University

Description

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

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

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

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

5. Schwab Charitable: See description of access or storage provided in the 2014 annual PIIDPA report.

6. Ruffalo Cody: See description of access or storage provided in the 2014 annual PIIDPA report.

7. Qualtrics: See description of access or storage provided in the 2014 annual PIIDPA report.

8. Saint Mary’s University Commercial Card Program: See description of access or storage provided in the 2014 annual PIIDPA report.

9. Evernote: Evernote is a cross-platform app designed for note taking, organizing, and archiving. Evernote is an independent, privately held company headquartered at Evernote Corporation, 305 Walnut Street Redwood City, California founded in 2007.

10. DropBox: File hosting service operated by DropBox, Inc, headquartered in San Francisco, California that offers cloud storage, file synchronization, personal cloud and client software. Dropbox allows users to create a special folder on their computers, which Dropbox then synchronizes so that it appears to be the same folder (with the same contents) regardless of which device is used to view it. Files placed in this folder are also accessible via the Dropbox website and mobile apps. Dropbox uses a freemium business model, wherein users are offered a free account with a set storage size and paid subscriptions for accounts with more capacity.

11. Go To Meeting/Go To Webinar: Online conferencing software with corporate headquarters located in Santa Clara, California, USA.

Conditions

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

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

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

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

5. Schwab Charitable: See conditions of access or storage provided in the 2014 annual PIIDPA report.

6. Ruffalo Cody: See conditions of access or storage provided in the 2014 annual PIIDPA report.

7. Qualtrics: See conditions of access or storage provided in the 2014 annual PIIDPA report.

8. Saint Mary's University Commercial Card Program: See conditions of access or storage provided in the 2014 annual PIIDPA report.

9. Evernote: Name and email address are required to create an account. All note files are saved in a folder attached to the user name in an Evernote database. Activity/ log files are saved to local drive.

10. DropBox: Cipher encryption for file data in transit and at rest, file segmentation and hashing to anonymize files. Teams can secure accounts even further with authentication features like single sign-on (SSO) support and two-step verification. Personal information like your name, email address, phone number, payment info, and physical address are used to associate with your account.

11. Go To Meeting/Go To Webinar: Users must log in with name and e-mail address.

Reasons

1. Plagiarism Detection: See reasons for access or storage provided in the 2012 annual PIIDPA report.

2. Maintenance Management System: See reasons for access or storage provided in the 2012 annual PIIDPA report.

3. Travel: See reasons for access or storage provided in the 2012 annual PIIDPA report.

4. Facilities Asset Management System: See reasons for access or storage provided in the 2012 annual PIIDPA report.

5. Schwab Charitable: See reasons for access or storage provided in the 2014 annual PIIDPA report.

6. Ruffalo Cody: See reasons for access or storage provided in the 2014 annual PIIDPA report.

7. Qualtrics: See reasons for of access or storage provided in the 2014 annual PIIDPA report.

8. Saint Mary's University Commercial Card Program: See reasons for access or storage provided in the 2014 annual PIIDPA report.

9. Evernote: Upgrade from free on-line service to subscription to increase upload limit, faster word recognition in images, heightened security, PDF annotation, Context, where notes and news articles can be seen, which are related to the open note and the ability to search text within PDF

documents. Used for collaborative communication across disciplines by team members for document collection and sharing.

10. DropBox: Used for collaborative communication across disciplines by team members for document collection and sharing.

11. Go To Meeting/Go To Webinar: This is an international product, allowing people from all over the world enrolled in our graduate programs to access information sessions.

Université Sainte-Anne

Description

1. Blackbaud: Student information system that has information stored in Boston, Mass. The storage is not offered in Canada.

2. MOODLE: Moodle is our course management system. Professors and students access this system to offer/access course content.

3. Email: Our e-mail system is housed on servers in Nova Scotia. Employees and student that travel internationally can access the e-mail system via smartphone, computer, or tablet.

Conditions

1. Password protected. No one in the US is to have access to personal information, unless required by law enforcement.

2. Professors and students access course information that is stored in NS, Canada on our server via computer and the access is password protected

3. Access is restricted via password protection.

Reasons

1. Access: A legal opinion was obtained to ensure that the storage arrangement met all PIIDPA's requirements.

2. Access is necessary in order to offer/receive course content that is required in order to achieve course requirements.

3. Employees and students require access to the e-mail system in order to assure the daily operations of the university, including course offerings.

University of King's College

Description

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

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

3. University ID Card. Management of access and financial processes used through the University ID Card.

4. Network and Systems Upgrades. Consulting services related to the University's ongoing upgrade of its internal network and systems.

5. Teaching and Research Statistical Software. Maintenance support for statistical software product used in course teaching and research (remote access from US).

6. Degree Progress Software. Maintenance support for academic product which provides students with information regarding their progress towards meeting their degree requirements (remote access from US).

7. Student Advising Scheduling Software. Maintenance support for a scheduling and data tracking software designed for university student advising and counseling (remote access from US).

8. Plagiarism Detection. Academic program: online plagiarism detection service (storage in US).

9. Undergraduate Student Survey. Student survey to measure student athletic facilities experiences.

10. Hosted Learning Management System. Academic product used extensively by faculty for online teaching.

11. Residence application database. Hosted by a US company.

12. Service provider maintenance (Konica Minolta hardware and software). Lease and maintenance multifunction devices (copy/print/scan/fax devices). Vendor headquartered in Japan.

13. Maintenance management software: MicroMain software provided by an American vendor, MicroMain Corporation. Data is stored in US-based cloud system.

14. Alumni/donor database: See description of access or storage provided in the 2014 annual PIIDPA report.

15. Conference management software: See description of access or storage provided in the 2014 annual PIIDPA report.

16. Journalism internships: See description of access or storage provided in the 2014 annual PIIDPA report.

17. Employee access to personal information from outside of Canada: See description of access or storage provided in the 2014 annual PIIDPA report.

Conditions

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

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

3. University ID Card. Limited access: only where required for maintenance and troubleshooting. Contractual security measures: all personal information will be stored in Canada; restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to university protocols including time restrictions, audit function and pre-approved IP addresses; removal of personal information prior to return of hardware where possible. The company has a support technician located in Canada who provides support whenever possible.

4. Network and Systems Upgrades. Limited access: only where required for maintenance and troubleshooting. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to university protocols including time restrictions, audit functions and pre-approved IP addresses.

5. Teaching and Research Statistical Software. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to university protocols including time restrictions, audit function and pre-approved IP addresses. Access to personal information for maintenance purposes will rarely, if ever, be required: research using this product will rarely ever contain personal information and dummy data can be created to illustrate a problem for maintenance purposes.

6. Degree Progress Software. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university systems will be subject to university protocols including time restrictions, audit function and pre-approved IP addresses.

7. Student Advising Scheduling Software. Contractual security measures: restrictions on access to and disclosure of information by service provider and employees; remote access to university

systems will be subject to university protocols including time restrictions, audit function and pre-approved IP addresses.

8. Plagiarism Detection. Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; storage of university information will be segregated from other users; internal security measures: process in place to minimize disclosure of personal information.

9. Undergraduate Student Survey. Technical security measures: data security controls in place; Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; Internal security measures: process in place to minimize disclosure of personal information.

10. Hosted Learning Management System. Technical security measures: data security controls in place; Contractual security measures: restrictions on access to and disclosure of information by service provider and their employees; Internal security measures: process in place to minimize disclosure of personal information.

11. Residence application database. Data is stored on a Canadian server and maintenance is performed by a local IT company.

12. Service provider maintenance (Konica Minolta hardware and software). The information collected is user specific. No print or user data is collected. The OPS Data Collection Agent uses an HTTPS connection to communicate with the agent control server. The OPS Data Collection Agent initiates all outgoing connections; no server ports are opened at the agent level. The agent control servers are secured against unauthorized access and will validate all incoming agent communication requests for a valid, unexpired registration key. The OPS Data Collection Agent uses secure HTTPS communication when connecting to the Canadian control server. Additionally, all end-user access to the application is encrypted using SSL (the OPS Data Collection Agent is not end-user accessible). Un-encrypted SNMP traffic is restricted to the local subnets the agent is configured to monitor. The information is stored on the server residing in Konica Minolta's facilities in Canada. No confidential information can be accessed by third parties outside of Canada.

13. Maintenance Management Software: MicroMain. The personal data being stored in this US-based cloud system is restricted to King's employees. Limited supervised remote access only where required for maintenance and troubleshooting.

14. Alumni/donor database: See conditions of access or storage provided in the 2014 annual PIIDPA report.

15. Conference management software: See conditions of access or storage provided in the 2014 annual PIIDPA report.

16. Journalism internships: See conditions of access or storage provided in the 2014 annual PIIDPA report.

17. Employee access to personal information from outside of Canada: See conditions of access or storage provided in the 2014 annual PIIDPA report.

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.

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

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

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

3. University ID Card. This system is proprietary in nature and is only sold and supported by this company. The University's identification card is used by all staff, faculty and students for a variety of purposes including access to facilities, financial transactions on and off campus and various administrative functions. Proper management of this integrated tool is necessary for the administrative function of the University.

4. Network and Systems Upgrades. Consultant services, provided by the current provider of the systems, are being upgraded and thus have the expertise to provide the services required. These systems are necessary for the operation of integral University computing services.

5. Teaching and Research Statistical Software. Necessary for University academic and research operations in several departments. This product offers superior functionality and range of service according to evaluations conducted by users; access rarely required.

6. Degree Progress Software. Allowing students to access their information regarding progress towards degree requirements is necessary for University operations particularly in student advising and counseling and for the Registrar's Office. No Canadian alternatives have been identified; access rarely required.

7. Student Advising Scheduling Software. Providing advising and counseling services to students and effectively managing and tracking those services is necessary for University student services operations. This product offers superior functionality and range of services; access rarely required.

8. Plagiarism Detection. Necessary for University academic programs in order to maintain high standards of academic integrity. There is currently no product in Canada offering a comparable range of service and functionality. Minimal personal information disclosed.

9. Undergraduate Student Survey. Necessary to assess the quality of athletic services delivered to students and compare to other Canadian schools. There is currently no comparable product offered in Canada. Data security controls in place. Minimal personal information disclosed.

10. Hosted Learning Management System. The provision of online teaching opportunities is necessary to University academic operations. This product offers a superior range of service and functionality; and has been an established service at the university for several years, therefore, would require a heavy cost to convert. Data security controls in place. Minimal personal information disclosed.

11. Residence application database. Data is stored in Canada and maintenance is performed by a Canadian IT firm in the presence of residence staff.

12. Service provider maintenance (Konica Minolta hardware and software). Awarded through a tender process.

13. Maintenance Management Software: MicroMain. King's has determined that security and privacy provided by the vendor meets the needs of the University. Determined to be the best fit for King's needs and is widely used by universities in Canada.

14. Alumni/donor database: See restrictions of access or storage provided in the 2014 annual PIIDPA report.

15. Conference management software: See restrictions of access or storage provided in the 2014 annual PIIDPA report.

16. Journalism internships: See restrictions of access or storage provided in the 2014 annual PIIDPA report.

17. Employee access to personal information from outside of Canada: See restrictions of access or storage provided in the 2014 annual PIIDPA report.

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[12]

Annapolis Valley Regional School Board

Description

1. Travel with electronic devices: Two AVRSB staff members travelled outside of Canada for business. They had the ability to access personal information contained in email or stored in the Microsoft Outlook email system using devices including cell phones, iPads/tablets and laptop computers. Staff must seek permission from the head of the public body before taking devices and personal information across the Canadian border.

2. Use of social media: AVRSB and a number of its schools operate a Twitter account. Twitter is based in the United States. These accounts are used for sharing news releases, videos, photos and other information to a broader audience.

3. Khan Academy: Khan Academy resources and interactive lessons are available on a variety of subjects, including mathematics, computer programming, 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. Personal information about students and teachers will be accessed and stored outside Canada as the Khan Academy is located outside Canada.

4. Advanced Placement: AVRSB has students who are enrolled in the Advanced Placement (AP) program administered by The College Board. Personal information including name, school attended, grade, and academic achievement is disclosed by the School Board to the College Board to administer the program.

5. Google Apps for Education: AVRSB students, teachers and administrators use Google Apps for Education, including services such as Drive, Sites, Gmail, Calendar, Groups and Contacts. Users may create, store online, and share documents, presentations, spreadsheets, etc. as well as domain exclusive web sites that can be shared with both internal and external users. The service can also provide a complete email, calendar and contacts function that can be configured for an educational domain of choice.

6. Aesop System: AVRSB uses 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. FPT requires periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.

[12] Atlantic Provinces Special Education Authority did not submit a PIIDPA Form 1.

7. International Baccalaureate Diploma Program: AVRSB has students who are enrolled in the International Baccalaureate (IB) program. Personal information including name, school attended, grade, and academic achievement is disclosed by the School Board to the IB administration to administer the program.

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. AVRSB and a number of its schools use Twitter to share information and interact online with the public and organizations in social spaces. AVRSB and its schools collect no IP addresses or personal information through these services. AVRSB retweets other government and school accounts and information from partners (RCMP, municipality, other school boards, etc.) Photos and videos that are posted to Twitter have written consent from the people in them where required.

3. It is recommended that teachers set up Khan Academy student accounts for students who 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 fictitious or a combination of three initials and five to six numbers, to reduce the ability to easily identify an individual, their gender, or ethnicity.

4. Parents/guardians receive information about the AP program, including that it is administered outside Canada through offices in New York State, USA.

5. Risk mitigation strategies are in place to reduce risks to personal information, including educating students and staff about the risks of providing or storing personal information in a cloud service such as Google Apps for Education, establishing policies to discourage the use of these services for sensitive or confidential purposes, and use of the Google Dashboard to see what information is collected and associated with their online identity.

6. The Department of Education and Early Childhood Development and AVRSB have signed a contract extension through June of 2018 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 PIIDPA. 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. Frontline's SunGard data 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 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.

7. Parents/guardians receive information about the IB program, including that it is administered outside Canada through offices in Switzerland and the United Kingdom.

Reasons

1. Staff are expected to monitor their email and voicemail for business continuity purposes. Cell phones were necessary to access email and internet sites, and to make telephone calls. Laptops and tablets 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.

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. Such access and storage is authorized through determination of 'necessity' under S. 5(2) of PIIDPA.

4. The AP program is available to Nova Scotia high school students as an option to regular studies or the IB. The AP program is administered by The College Board, a not-for-profit organization in New York. AP courses give students access to rigorous college-level work. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

5. Google Apps for Education is a productivity tool used by all school boards that supports and encourages collaboration among teachers and students. This tool assists in supporting 21st century learning skills and competencies. The ubiquitous access via virtually any internet-connected device expands opportunities for teachers and students to access these resources both within and outside the school and provides a measure of equity for all.

6. 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.

7. The IB program is available to Nova Scotia high school students as an option to regular studies or the Advanced Placement program. It challenges students to excel in their studies, and encourages both personal and academic achievement. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

Cape Breton-Victoria Regional School Board

Description

1. The School Board along with several schools operates a Twitter account. Twitter is based in the United States. These accounts are used for sharing School Board news releases, videos, photos and other information to a broader audience.

2. The Cape Breton-Victoria 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. Khan Academy was partnered with Hour of Code and Code.org which was also endorsed by the DEECD. Khan Academy resources and interactive lessons are available on a variety of subjects, including mathematics, computer programming, 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. Personal information about students and teachers will be accessed and stored outside Canada as the Khan Academy is located outside Canada.

4. The Cape-Breton-Victoria Regional School Board has students who are enrolled in the International Baccalaureate program. Personal information including name, school attended, grade, and academic achievement was disclosed by the School Board to the IB to administer the program.

Conditions

1. The School Board administration and schools use Twitter to share information and interact online with the public and organizations in social spaces. The School Board and schools collect no IP addresses or personal information through these services. The School Board and schools retweet other School Boards, schools, government accounts and public safety information from partners (RCMP, municipality, school boards, universities, etc.).

2. The Cape Breton-Victoria 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. It is recommended that teachers set up Khan Academy student accounts for students who 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.

4. Parents/guardians receive information about the IB program, including that it is administered outside Canada (Switzerland, UK, etc.).

Reasons

1. 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.

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

3. 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. Such access and storage is authorized through determination of "necessity" under S. 5(2) of PIIDPA.

4. The IB program is available to Nova Scotia high school students as an option to regular studies or the Advanced Placement program. It challenges students to excel in their studies, and encourages both personal and academic achievement. The program provides an internationally accepted qualifications for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

Chignecto-Central Regional School Board

Description

1. Travel with Electronic Devices: See description of access and/or storage provided in the 2014 annual PIIDPA report.

2. Use of Social Media: See description of access and/or storage provided in the 2014 annual PIIDPA report.

3. AESOP: See Description of access and or storage provided in the 2014 annual PIIDPA report..

4. Future Goals - Hockey Scholar by Everfi: The tool will be used by teachers and students (recommended for grades 5 to 7). It is supported by CCRSB Mathematics Program and it is a highly motivational and engaging resource that uses performance-based games. There is no known similar alternative.

5. World Math Day: It is an online international mathematics competition. Alternatives are not as user friendly or require a cost. This service is free. It involves students playing 60 second games.

6. Plickers: The use of Plickers will support student engagement and allow for collection of useful assessment data. It allows for students to respond without feeling peer pressure. Teachers can use the information gathered and share class results or discuss individual results with students.

7. KidblogIt: KidblogIt allows student to publish their work in a moderated environment and allows for feedback from an authentic audience. Basic enrolment is free.

Conditions

1. Same as above.

2. Same as above.

3. Same as above.

4. The Privacy Policy states that Everfi does not sell [students'] personal information, and a [student] may not make his or her personal information public through their services. In general, they may disclose the personal information that they collect about [students] to provide our services, to comply with the law, and to protect Everfi and other users of our services.

5. Students will not be creating their own accounts. It will be recommended that a printed alternative be made available for any families wishing to use it.

6. The personal information shared is of a very limited nature. Teachers will be provided guidance as to what is appropriate information to include.

7. Teachers and students may post pictures or student work if the media release form has been signed by parents or guardians. The only information required is a student display name.

Reasons

1. Same as above.

2. Same as above.

3. Same as above.

4. First names are required but information provided could be fictitious. Students will be working on this within the school environment and therefore the normal classroom practices will ensure equity.

5. The privacy policy states that 3P Learning will keep personal information confidential and not sell or knowingly divulge information to advertisers or any external third parties except under specific conditions listed on the site. The site has developed in its policy accordance with the Alberta Freedom of Information and Protection of Privacy Act and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) amongst others.

6. Student use is paper-based and therefore equity is not an issue. Teachers can create student display names that are not related to their name or any other personal information.

7. Kidblog will make commercially reasonable efforts to safeguard the information submitted. The personal information is very limited.

Conseil Scolaire Acadien Provincial

Description

1. A number of CSAP staff members traveled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in the Microsoft Outlook email system using devices including smart phones, tablets and laptops. The board approved six (6) school trips outside Canada for a variety of learning experiences.

2. Some CSAP schools are in the testing phase of Alert Solution (auto-dialer) to send messages to parents and staff instantly and reliably.

3. Some CSAP schools have access to the Khan Academy resources and interactive lessons.

4. CSAP and several of its schools operate Twitter accounts for sharing government news releases, videos, photos and other information to a broader audience.

5. Some CSAP schools have online subscriptions for education media Learning A-Z.

6. CSAP and all schools utilize an on-line SchoolCash system provided by KEV Group for the management of school activity funds.

7. CSAP and all schools utilize the provincial SAP system finance, human resources, procurement and operations.

8. CSAP and all schools utilize the provincial Student Information System (SIS) and TIENET to manage student documentation.

9. CSAP is in the testing phase of the Aesop system provided by FrontLine Technologies Canada for tracking, processing and storing information related to employee absences.

Conditions

1. See details provided in the 2014 annual PIIDPA report under Conseil scolaire acadien provincial.

2. See details provided in the 2014 annual PIIDPA report under Education and Early Childhood Development.

3. See details provided in the 2014 annual PIIDPA report under South Shore Regional School Board.

4. See details provided in the 2014 annual PIIDPA report under Conseil scolaire acadien provincial.

5. See details provided in the 2013 annual PIIDPA report under Conseil scolaire acadien provincial.

6. See details provided in the 2013 annual PIIDPA report under Conseil scolaire acadien provincial.

7. See details provided in the 2013 annual PIIDPA report under Finance and Treasury Board.

8. See details provided in the 2014 annual PIIDPA report under Education and Early Childhood Development.

9. See details provided in the 2014 annual PIIDPA report under Cape-Breton Regional School Board.

Reasons

1. See details provided in the 2014 annual PIIDPA report under Conseil scolaire acadien provincial.
2. See details provided in the 2014 annual PIIDPA report under Education and Early Childhood Development.
3. See details provided in the 2014 annual PIIDPA report under South Shore Regional School Board.
4. See details provided in the 2014 annual PIIDPA report under Conseil scolaire acadien provincial.
5. See details provided in the 2013 annual PIIDPA report under Conseil scolaire acadien provincial.
6. See details provided in the 2013 annual PIIDPA report under Conseil scolaire acadien provincial.
7. See details provided in the 2013 annual PIIDPA report under Finance and Treasury Board.
8. See details provided in the 2014 annual PIIDPA report under Education and Early Childhood Development.
9. See details provided in the 2014 annual PIIDPA report under Cape-Breton Regional School Board.

Halifax Regional School Board

Description

1. Travel with electronic devices - Eighteen (18) Halifax Regional School Board staff traveled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in the Microsoft Outlook email system, using devices including cell phones, iPads, laptops, etc. Staff seeks 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 HRSB 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. YouTube – The HRSB uses also uses YouTube as a professional communication tool to engage the school community and share relevant information to parents, teachers, students and the public. YouTube is based in the United States.

3. Khan Academy - Khan Academy resources and interactive lessons are available on a variety of subjects, including mathematics, computer programming, 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.

Personal information about students and teachers will be accessed and stored outside Canada as the Khan Academy is located outside Canada.

4. Google Apps for Education - The Halifax Regional School Board's students, teachers and administrators use Google Apps for Education, including services such as Drive, Sites, Gmail, Calendar, Groups and Contacts. Users may create, store online, and share documents, presentations, spreadsheets, etc., as well as domain exclusive web sites that can be shared with both internal and external users. The service can also provide a complete email, calendar and contacts function that can be configured for an educational domain of choice.

5. Aesop - The Halifax 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. International Baccalaureate Diploma Program - The Halifax Regional School Board has students who are enrolled in the International Baccalaureate program. Personal information including name, school attended, grade, and academic achievement is disclosed by the School Board to the IB to administer the program.

7. Advanced Placement - The Halifax Regional School Board has students who are enrolled in the Advanced Placement program administered by The College Board. Personal information including name, school attended, grade, and academic achievement is disclosed by the School Board to the College Board to administer the program.

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. Use of Social Media -

    a. The HRSB uses Twitter to share information and interact online with the public and organizations in social spaces. The HRSB collects no IP addresses or personal information through these services. The HRSB 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.

3. It is recommended that teachers set up Khan Academy student accounts for students who 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.

4. Risk mitigation strategies are in place to reduce risks to personal information, including educating students and staff about the risks of providing or storing personal information in a cloud service such as Google Apps for Education, establishing policies to discourage the use of these services for sensitive or confidential purposes, and use of the Google Dashboard to see what information is collected and associated with their online identity.

5. The Department of Education and Early Childhood Development and the Halifax 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.

   Aesop's storage 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 Halifax 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. Parents/guardians receive information about the IB program, including that it is administered outside Canada (Switzerland, UK, etc.).

7. Parents/guardians receive information about the AP program, including that it is administered outside Canada (New York, USA).

<u>Reasons</u>

1. Staff is expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. Cell phones were necessary to make calls, access email and internet sites, and make telephone calls. Laptops and other devices 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 YouTube.

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. Such access and storage is authorized through determination of “necessity” under S. 5(2) of PIIDPA.

4. Google Apps for Education is a productivity tool used by all school boards that supports and encourages collaboration among teachers and students. This tool assists in supporting 21st century learning skills and competencies. The ubiquitous access via virtually any internet-connected device expands opportunities for teachers and students to access these resources both within and outside the school and provides a measure of equity for all.

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. The IB program is available to Nova Scotia high school students as an option to regular studies or the Advanced Placement program. It challenges students to excel in their studies, and encourages both personal and academic achievement. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

7. The AP program is available to Nova Scotia high school students as an option to regular studies or the IB. The AP program is administered by The College Board, a not-for-profit organization in New York. AP courses give students access to rigorous college-level work. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

South Shore Regional School Board

Description

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

2. Use of Social Media –

   a. Twitter - The South Shore Regional School Board operate as 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 South Shore Regional School Board 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.

8. Khan Academy - Khan Academy resources and interactive lessons are available on a variety of subjects, including mathematics, computer programming, 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.

   Personal information about students and teachers will be accessed and stored outside Canada as the Khan Academy is located outside Canada.

3. Google Apps for Education - The South Shore Regional School Board's students, teachers and administrators use Google Apps for Education, including services such as Drive, Sites, Gmail, Calendar, Groups and Contacts. Users may create, store online, and share documents, presentations, spreadsheets, etc. as well as domain exclusive web sites that can be shared with both internal and external users. The service can also provide a complete email, calendar and contacts function that can be configured for an educational domain of choice.

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.

5. International Baccalaureate Diploma Program - The South Shore Regional School Board has students who are enrolled in the International Baccalaureate. Personal information including name, school attended, grade, and academic achievement is disclosed by the School Board to the IB program to administer the program.

6. Advanced Placement - The South Shore Regional School Board has students who are enrolled in the Advanced Placement program administered by The College Board. Personal information including name, school attended, grade, and academic achievement is disclosed by the School Board to the College Board to administer the program.

Conditions

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

2. Use of Social Media –

   a. The South Shore Regional School Board uses Twitter to share information and interact online with the public and organizations in social spaces. The South Shore Regional School Board collects no IP addresses or personal information through these services. The South Shore Regional School Board 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 on all social media platforms have written consent from the people in them, where required.

3. It is recommended that teachers set up Khan Academy student accounts for students who 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.

4. Risk mitigation strategies are in place to reduce risks to personal information, including educating students and staff about the risks of providing or storing personal information in a cloud service such as Google Apps for Education, establishing policies to discourage the use of these services for sensitive or confidential purposes, and use of the Google Dashboard to see what information is collected and associated with their online identity.

5. The Department of Education and Early Childhood Development and the South Shore Regional School Board have signed a contract extension through June of 2018 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 data facility in Toronto, Ontario, 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

1. Parents/guardians receive information about the IB program, including that it is administered outside Canada (Switzerland, UK, etc.).

2. Parents/guardians receive information about the AP program, including that it is administered outside Canada (New York, USA).

Reasons

1. Staff are expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. Cell phones were necessary to make calls, access email and internet sites. Laptops and other devices 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 YouTube.

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. Such access and storage is authorized through determination of “necessity” under S. 5(2) of PIIDPA.

8. Google Apps for Education is a productivity tool used by all school boards that supports and encourages collaboration among teachers and students. This tool assists in supporting 21st century learning skills and competencies. The ubiquitous access via virtually any internet-connected device expands opportunities for teachers and students to access these resources both within and outside the school and provides a measure of equity for all.

9. FPT’s Aesop system is functionally superior compared 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".

10. The IB program is available to Nova Scotia high school students as an option to regular studies or the Advanced Placement program. It challenges students to excel in their studies, and encourages both personal and academic achievement. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

11. The AP program is available to Nova Scotia high school students as an option to regular studies or the IB program. The AP program is administered by The College Board, a not-for-profit organization in New York, NY. AP courses give students access to rigorous college-level work. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

Strait Regional School Board

Description

1. Travel with electronic devices - A number of Strait Regional School Board staff traveled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in the IBM Lotus Notes email system, using devices including personal cell

phones, iPads, laptops, etc. 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 Strait Regional School Board operate as a Twitter account. Fifteen schools (15) under the jurisdiction of the Strait 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.

   b. Facebook – The Strait Regional School Board does not operate a Facebook account. Four (4) schools under the jurisdiction of the Strait Regional School Board 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.

3. Google Apps for Education - The Strait Regional School Board's students, teachers and administrators use Google Apps for Education, including services such as Drive, Sites, Gmail, Calendar, Groups and Contacts. Users may create, store online, and share documents, presentations, spreadsheets, etc. as well domain exclusive web sites that can be shared with both internal and external users. The service can also provide a complete email, calendar and contacts function that can be configured for an educational domain of choice.

4. Aesop - 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.

5. International Baccalaureate Diploma Program - The Strait Regional School Board has students who are enrolled in the International Baccalaureate program. Personal information including name, school attended, grade, and academic achievement is disclosed by the School Board to the IB program to administer the program.

6. Raz Kids - The Strait Regional School Board has students enrolled in Raz Kids which is mainly used by teachers to supplement reading. It is used in nearly half of the school districts in the US, Canada and 155+ countries worldwide.

7. Mathletics - Mathletics is an online learning platform, helping students enjoy math and improve their results. It can be used on a computer or tablet.

8. IXL - IXL is very similar to Mathletics. It is on-line, individualized by students where they can practice Math skills from Primary to Grade 12 and receive reports on their progress. Skills are aligned to the Nova Scotia Curriculum.

Conditions

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

2. Use of Social Media –

    a. The Strait Regional School Board and fifteen (15) schools use Twitter to share information and interact online with the public and organizations in social spaces. The Strait Regional School Board collects no IP addresses or personal information through these services. The Strait Regional School Board re-tweets other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.).

    b. The schools post 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 on all social media platforms have written consent from the people in them, where required.

3. Risk mitigation strategies are in place to reduce risks to personal information, including educating students and staff about the risks of providing or storing personal information in a cloud service such as Google Apps for Education, establishing policies to discourage the use of these services for sensitive or confidential purposes, and use of the Google Dashboard to see what information is collected and associated with their online identity.

4. The Department of Education and Early Childhood Development and the Strait Regional School Board have signed a contract extension through June of 2018 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 data 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 School Board are provided access to the Board’s electronic information. The data contained in the system is limited to that required to ensure successful operation.

    Parents/guardians receive information about the IB program, including that it is administered outside Canada (Switzerland, UK, etc.)

Reasons

1. Staff is expected to monitor their email for business continuity purposes, and maintain contact with operations. Permission to take Board-owned cell phones was granted on several occasions and

was necessary to make calls and access email. Board-owned laptops and other board-owned devices were not permitted across the Canadian border.

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. Google Apps for Education is a productivity tool used by all school boards that supports and encourages collaboration among teachers and students. This tool assists in supporting 21st century learning skills and competencies. The ubiquitous access via virtually any internet-connected device expands opportunities for teachers and students to access these resources both within and outside the school and provides a measure of equity for all.

4. 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".

5. The IB program is available to Nova Scotia high school students as an option to regular studies or the Advanced Placement program. It challenges students to excel in their studies, and encourages both personal and academic achievement. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

6. Personal information of students is not shared. An identifier is provided by the teacher (i.e. number of initials).

7. In some cases, students' real names are not used; only initials or identifier/numbers or both. In other cases, written parental permission is sought.

8. Students' real names are not used; only initials or identifier/numbers or both. In other cases, written parental permission is sought.

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 on 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 for students who 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 compared to other systems on the market and it represents a 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[13,14]

Cape Breton Regional Municipality [15]

Description

1. We currently do not allow our data to be stored outside the country.

2. There were 23 occasions where CBRM employees travelled outside of the country with a CBRM device, such as a laptop, smart phone, or tablet.

Restrictions

1. All data storage is within Canada, therefore no restrictions were necessary.

2. We do require each employee that is taking a CBRM device (e.g., laptop, smart phone, tablet) outside the country to register the dates they are travelling, along with the country to the Department of Technology (started in September 2015).

Conditions

1. It is a practise for the CBRM not to store data outside the country, therefore this is not an issue for storage of data.

2. Employees taking CBRM devices (e.g., laptops, smart phones, tablets) outside of the country on occasion are required to register with the Department of Technology.

[13] Municipality of the County of Antigonish, Municipality of the County of Cumberland, Municipality of the County of Kings, Municipality of the County of Richmond, Municipality of the County of Victoria, 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 County of Victoria, Municipality of the District of St. Mary's, Municipality of the District of Shelburne (includes the Shared Services Board), Region of Queens Municipality, Town of Antigonish, Town of Berwick, Town of Lockeport, Town of Lunenburg, Town of Mahone Bay, Town of Pictou, Town of Port Hawkesbury, Town of Shelburne, Town of Stellarton, Town of Stewiacke, Town of Trenton, Town of Truro, Town of Westville, Town of Windsor, Town of Yarmouth, and the Cumberland Joint Services Management Authority did not have access or storage outside of Canada to report.

[14] Digby Area Recreation Commission, South Shore Regional Library Board, Town of Clark's Harbour, Town of Kentville, Town of Middleton, Town of Mulgrave, Town of New Glasgow, Town of Oxford, Town of Parrsboro did not provide a completed PIIDPA Form 1.

[15] Report includes Cape Breton Regional Police Service

Halifax Regional Municipality[16]

Description

1. Between January 1st and December 31st, 2015, sixty-two (62) HRM staff and nine (9) 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, Environmental Health & Safety Management 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. 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.

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

[16] Report includes Halifax Regional Police and the Halifax Public Library

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

13. Fluid Surveys (obtained by Survey Monkey), with a Canadian headquarters in Ottawa, ON, HRM's data is hosted in Canada.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

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

20. 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.

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

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

23. Service Providers - Kenexa - Brassring, HR Applicant Tracking System and Skills Assessment Tool, with a headquarters in Wayne, PA.

24. Service Provider - Explore Analytics, with a headquarters in San Jose, CA.

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

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

27. 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.

28. Service Provider - Active Network - Hosted Payment Server - with a headquarters in Las Vegas, NV.

Conditions

1. Prior to travelling, staff were advised that HRM Communication tools (e.g., cell phones, smart phones, laptops, memory sticks, VPN) were to be password protected.

2. Vendor access is controlled and monitored by ICT Support staff.

3. Vendor access is controlled and monitored by ICT Support staff.

4. Vendor access is controlled and monitored by ICT Support staff.

5. Vendor access is controlled and monitored by ICT Support staff.

6. Vendor access is controlled and monitored by ICT Support staff.

7. Vendor access is controlled and monitored by ICT Support staff.

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

9. Vendor access is controlled and monitored by ICT Support staff.

10. Vendor access is controlled and monitored by ICT Support staff.

11. Vendor access is controlled and monitored by ICT Support staff

12. Vendor access is controlled and monitored by ICT Support staff.

13. Vendor access is controlled and monitored by ICT Support staff.

14. Vendor access is controlled and monitored by ICT Support staff.

15. Vendor access is controlled and monitored by ICT Support staff.

16. Vendor access is controlled and monitored by ICT Support staff.

17. Vendor access is controlled and monitored by ICT Support staff.

18. Vendor access is controlled and monitored by ICT Support staff.

19. Vendor access is controlled and monitored by ICT Support staff.

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

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

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

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

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

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

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

27. Vendor access is controlled and monitored by ICT Support staff.

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

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

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

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

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

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

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

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

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

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

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

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

13. 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.

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

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

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

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

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

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

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

21. 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.

22. 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.

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

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. 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.

26. 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.

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

28. Class software (Active Networks) has been used by the municipality for 15+ years to manage recreational programs. The addition of the hosted payment server will allow the processing of Class payments in a PCI compliant manner.

Halifax Regional Water Commission

Description

1. Between January 1 and December 31, 2015, forty-five (45) Halifax Water staff were permitted to transport personal information devices, such as laptop computers, cell phones, and electronic data storage devices outside Canada seventy-two (72) 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 Regional Water Commission communication tools (e.g., cell phones, blackberries, laptops, memory sticks, VPN) are to be used for operational requirements only and were to be password protected.

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

Reasons

1. Halifax Regional Water Commission 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 Annapolis[17]

Description

1. From August 13 to 21, 2015, the Warden travelled outside of Canada on official County business. He took a municipally-owned smartphone with him to access his municipal e-mail account.

Conditions

1. All e-mail access was through a centrally managed Blackberry or iPhone device.

Reasons

1. The information accessed in all cases was required for business purposes of the County of Annapolis. The Warden is required to have access to work e-mail in case of emergency work situations such as activation of our Regional Emergency Management Office.

Municipality of the County of Colchester

Description

1. See description of access and/or storage provided in the 2014 annual PIIDPA report.

[17] Report includes Planning, Public Works, Building Inspection Services, and Recreation and Finance Service Groups

Conditions

1. See description of access and/or storage provided in the 2014 annual PIIDPA report.

Reasons

1. See description of access and/or storage provided in the 2014 annual PIIDPA report.

Municipality of the County of Inverness

Description

1. There were five (5) instances where four (4) employees travelled outside of Canada. Each employee had an iPhone.

Conditions

1. The phones were password protected.

Reasons

1. Employees were travelling for work/and or personal reasons and required email access to stay connected with the Municipal Offices.

Municipality of the County of Pictou

Description

1. Employees within the Municipality of the County of Pictou travelled outside of Canada with their municipally-owned electronic device. Approval had been granted for the employees to take their devices with them. During this time, employees had access to the Municipality's email system from their mobile devices.

Conditions

1. All devices are encrypted and password protected, and are under the control of the Municipality's internal Enterprise Server. Remote access webmail is encrypted with SSL and protected usernames and passwords are changed on a regular basis.

Reasons

1. Employees or elected officials may request to travel out of the country with their municipally-owned devices. The Chief Administrative Officer has the final decision on whether an employee may take their device with them. The decision is based upon whether the employee, in their role with the municipality, is required to access information while they are away from the municipality.

Municipality of the County of Richmond

Description

1. One (1) management person travelled to the US for business purposes.

Conditions

1. Access to information was done through secure network access only. All devices are password protected.

Reasons

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

Municipality of the District of Chester

Description

1. Remote access via electronic devices such as iPhones, iPads and laptops. There were three (3) instances in which staff members were approved to take electronic devices while travelling outside Canada. During this time staff had access to the Municipality's email system from mobile devices.

Conditions

1. All devices are encrypted and password protected under Mobility Control Software. AES-256 encryption is used for VPN access.

Reasons

1. Required to meet operational demands when travelling with adequate security measures in place to secure all data. Devices could be remotely wiped if lost or stolen.

Municipality of the District of East Hants

Description

1. Constant Contact was deployed to communicate with East Hants stakeholders. Stakeholders were invited to subscribe to the service via the Municipal website, www.easthants.ca.

2. Wrike.com was deployed for effective project management. All content is accessed from and stored in the United States.

3. Dropbox.com was deployed for large file sharing. All content is accessed from and stored in the United States.

4. Access to information stored on Municipal servers was accessed via electronic devices in the United States by four (4) Councillors and one (1) senior staff member. Protection of privacy protocols are followed when accessing Municipal information.

5. The Municipality of East Hants has an agreement with U.S. Bank, Visa card provider. Total System 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 which would be stored is that which is provided by commercial card clients (e.g., name, address, telephone numbers, birth dates, employee numbers, etc.).

Conditions

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

2. N/A

3. N/A

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

5. "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. The storage of information on Constant Contact was necessary to conduct business in 2015. The Municipality of East Hants continues to explore other means of gathering and storing personal contact details.

2. The storage of information on Wrike.com was necessary to conduct business in 2015. The Municipality of East Hants continues to explore other means of collaborative project management tools.

3. The storage of information on dropbox.com was necessary to conduct business in 2015. The Municipality of East Hants continues to explore other means of large file sharing tools.

4. The access of information from mobile devices and laptops was necessary to conduct Municipal business while in the United States.

5. The U.S. Bank has been the service provider for the Municipality of East Hants for the past 16 years.

Municipality of the District of Guysborough

Description

1. Use of cellular phone for emergency office contact while on vacation (September 22 - 26, 2015); Director had phone and tablet while attending a conference (May 4 - 7, 2015); Use of cell phone while on vacation to remain in contact with department (December 1 - 8, 2015); and CAO to have contact back to main office with phone and tablet while attending a conference (May 4 - 7, 2015).

Conditions

1. Use only as necessary; Use only as a last resort; Use only as necessary; and Use only if necessary.

Reasons

1. Director who needs to have contact with their department; Director needed contact back with his department; Director needed to have contact back with their department; and CAO needs to have contact with main office.

Municipality of the District of Lunenburg

Description

1. Occasionally, the Municipality's data network is accessed by third parties in the provision of technical support. All such routine access is provided by vendors physically located in Canada. Special access by other support providers is allowed while supervised on an as-needed basis. The Municipality does not currently use any cloud-based services which are hosted outside of Canada.

2. Municipal property owners living outside of Canada are sent property tax invoices twice per year (April and September). There are often exchanges in communication via e-mail with these customers.

3. One (1) municipal elected official travelled outside of Canada and could have accessed personal e-mail through a municipally owned iPad. Appropriate permissions were granted.

   No municipal employees who travelled internationally for personal or pleasure reasons had access to MODL electronic equipment/devices or accessed MODL personal information.

Conditions

1. Vendor access is controlled and monitored by IT Support Systems.

2. All e-mail activity is controlled and monitored by our IT support.

3. Official was advised to limit the use of e-mail during the time out of the country. Prior to travelling, the user was instructed on how to access their e-mail and other services without any data actually being transmitted across the border. Secure login/passwords and/or encryption protocols were in place.

Reasons

1. Vendor access is necessary in the daily operations of the Municipality in order to continue business functions properly.

2. This is an operational process that occurs on a regular basis and provides for efficient manner for customer service.

3. The elected official was expected to maintain a means of communication with the business of the Municipality and to monitor e-mail in order to fulfill responsibilities/requirements.

Municipality of the District of West Hants

Description

1. Remote Access to information while traveling outside of Canada - Staff and Council are provided remote access to email and files stored at the West Hants offices. Primary access to email is provided through the use of iPhone and iPads for Municipal Councillors, and both a laptops and mobile devices for staff while travelling outside of Canada.

2. Access to Transient Data - Instances of municipal staff using cloud services to temporarily store files for the purposes of sharing with others and easily access data on multiple devices for meeting purposes. Services such as Dropbox and Google Drive are used from time to time to provide ease of access. This is not a permanent storage facility by any means, but a quick method to share files with parties outside the municipal organization. Staff do not store files permanently using these services.

Conditions

1. Mobile Devices (iPhone and iPad) - Access to email is provided via the internet, mobile devices are required to have a passcode to access the device. Remote wipe capabilities are in place for the administrator of IT network to remotely wipe any device that is lost or stolen. Also, unsuccessful passcode attempts will wipe device (e.g., after 10 unsuccessful log in attempts). Access to municipal data on mobile devices outside of email is provided by the use of a VPN data connection on an SSL SharePoint site. The IT administrator can revoke VPN access should the mobile device be lost or stolen. No municipal data (outside of email) is stored on the mobile device, access is through a VPN connection. Other Access: Access to municipal data via laptop computers is done through the use of a VPN connection or an SSL SharePoint Site. Laptops require a password to access email, VPN and documents stored on the municipal network at the municipal offices. Laptops are also password protected.

Reasons

1. Council and Staff are required to stay in contact with municipal operations while travelling outside of the country. The use of the VPN connection and password protected mobile devices allows that necessary level of access.

Municipality of the District of Yarmouth

Description

1. Five (5) employees travelled outside Canada and had the ability to access personal information via one or more of the following means: Smartphone and laptop.

Conditions

1. All devices were password protected and the laptop information was encrypted. Access to our network was done through secure services.

Reasons

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

Town of Amherst[18]

Description

1. Three (3) Town of Amherst staff travelled to the United States on personal time (vacation) in 2015 and had access to personal information (e.g., previous emails, email addresses) via Blackberry, iPhone or iPad. Prior approval to travel outside Canada with mobile devices was obtained from the CAO.

2. The Town of Amherst's human resource overtime, vacation and sick time information is stored within EZ Labour, a product offered by ADP.

Conditions

1. Email access requires authentication through secure login/password. If access is required, VPN is used to access electronic data remotely.

2. EZ Labour authentication is required through secure login/password.

Reasons

1. 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.

2. 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.

[18] Report includes Amherst Police Department

Town of Annapolis Royal[19]

Description

1. Since approximately 2003, the website for the Town of Annapolis Royal has been facilitated by a private firm which hosts the website in a reputable web host in Utah and Texas.

2. One (1) Municipal elected official travelled outside Canada and had the ability to access personal information via a tablet/cell phone device. Appropriate permissions were self-granted.

Conditions

1. The website does not contain any confidential or personal information that is not accessible for public use.

2. 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. The decision to allow the Town's website to go through Utah and Texas was made prior to my employment with the Town of Annapolis Royal. An overhaul of the website will be undertaken within the next couple of years and at that time consideration will be given to moving to a web host in Canada.

2. The Municipal official was expected to monitor email in order to fulfill responsibilities/requirements of duties.

Town of Bridgewater[20]

Description

1. Between January 1, 2015 to and including March 31, 2016, Four (4) Councillors (including one (1) councillor leaving the country 11 times), six (6) staff, and two (2) 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: cellphone, laptop, flashdrive, or Blackberry. However, only two (2) Councillors and two (2) staff accessed the Town of Bridgewater's server while out of the country. All were made aware of the requirements to access the town's server from afar and the majority chose to leave their devices at home and/or chose to "disengage" access to the town's information all together.

[19] Report includes Annapolis Royal Police Department and Town of Annapolis Royal Public Works.

[20] Report includes Bridgewater Police Services

Conditions

3. The Town of Bridgewater has had a Network Acceptable Use Policy (#61) in place since 2001. This policy includes requirements for the password protection of devices which may contain data, as well as reporting requirements for devices which are lost, stolen, or which the user has been compelled to provide a password at an international border. Equipment is available on loan for the purpose of international travel which has been certified free of personal data by Information Technology staff. In addition, the Town encourages users to use web-based access to their email while travelling, effectively maintaining the sovereignty of the data within Canada. Occasionally the Town data network is accessed by third parties in the provision of technical support. All such routine access is provided by vendors physically located in Canada. Special access by other support providers is allowed while supervised on an as-needed basis. The Town does not currently use any cloud-based services which are hosted outside of Canada.

Reasons

1. 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

1. The Mayor traveled to Europe for business purposes and had access to email through his cell phone.

Conditions

1. A password was maintained on the cell phone. No access to town files or other electronic information was available with the only exception being email and calendar appointments.

Reasons

1. 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 Organization.

Town of Kentville

Description

1. Two (2) Town of Kentville Councillors travelled to the United States in 2015, and accessed email via iPhone, iPad, and laptop. Prior approval to travel outside Canada with mobile devices was obtained from the CAO.

Conditions

1. Email access requires authentication through secure login/password. Councillors accessed a website that is hosted in Canada for meeting packages.

Reasons

1. Required to meet operational demands when travelling with adequate security measures in place to secure all data. All devices can be remotely accessed and wiped if required, if they are lost or stolen. Councillors used Skype to attend meetings electronically and the devices were needed for communication with the public body.

Town of Middleton

Description

1. Remote Access to information while traveling outside of Canada: Staff and Council are provided remote access to email and files stored at the Town of Middleton offices. Primary access to email is provided through the use of iPhone and iPads for Municipal Councillors, and both laptops and mobile devices for staff while travelling outside of Canada.

2. Access to Transient Data: Instances of municipal staff using cloud services to temporarily store files for the purposes of sharing with others and easily access data on multiple devices for meeting purposes. Services such as Dropbox and Google Drive are used from time to time to provide ease of access. This is not a permanent storage facility by any means, but a quick method to share files with parties outside the municipal organization. Staff do not store files permanently using these services.

Conditions

1. Mobile Devices (iPhone and iPad): Access to email is provided via the internet. Mobile devices are required to have a passcode to access the device. Remote wipe capabilities are in place for the administrator of IT network to remotely wipe any device that is lost or stolen. Also, unsuccessful passcode attempts will wipe device (e.g., after 10 unsuccessful log in attempts).

   Access to municipal data on mobile devices outside of email is provided by the use of a SSL data connection, though a secured password protected site, SharePoint. IT administrator can revoke access should the mobile device be lost or stolen. No municipal data (outside of email) is stored on the mobile device. Accesses are only through the SSL connection.

   Other Access: Access to municipal data via laptop computers is done through the use of a VPN connection. Laptops require a password to access email, VPN and documents stored on the municipal network at the municipal offices. Laptops are also password protected. Laptop can also access SharePoint through an SSL connection to SharePoint servers located in the Town of Middleton offices.

Reasons

1. Council and staff are required to stay in contact with municipal operations while travelling outside of the country. The use of the VPN connection and password protected mobile devices allows that necessary level of access.

Town of Wolfville

Description

1. Remote access to information while traveling outside of Canada - Staff and Council are provided remote access to email and files stored at the Town of Wolfville offices. Primary access to email is provided through the use of iPhone and iPads for Municipal Councillors, and both laptops and mobile devices for staff while travelling outside of Canada.

2. Access to Transient Data - Instances of municipal staff using cloud services to temporarily store files for the purposes of sharing with others and easily access data on multiple devices for meeting purposes. Services such as Dropbox and Google Drive are used from time to time to provide ease of access. This is not a permanent storage facility by any means, but a quick method to share files with parties outside the municipal organization. Staff do not store files permanently using these services

Conditions

1. Mobile Devices (iPhone and iPad): Access to email is provided via the internet. Mobile devices are required to have a passcode to access the device. Remote wipe capabilities are in place for administrator of IT network to remotely wipe any device that is lost or stolen. Also, unsuccessful passcode attempts will wipe device (e.g., after 10 unsuccessful log in attempts).

   Access to municipal data on mobile devices outside of email is provided by the use of a VPN data connection. The IT administrator can revoke VPN access should the mobile device be lost or stolen. No municipal data (outside of email) is stored on the mobile device. Accesses are only through the VPN connection.

   Other Access: Access to municipal data via laptop computers is done through the use of a VPN connection. Laptops require a password to access email, VPN and documents stored on the municipal network at the municipal offices. Laptops are also password protected.

Reasons

1. Council and staff are required to stay in contact with municipal operations while travelling outside of the country. The use of the VPN connection and password protected mobile devices allows that necessary level of access.

Foreign Access and Storage by Municipal Police

Stellarton Police Department, Truro Police Service and Westville Police Service did not have access or storage outside of Canada to report.

New Glasgow Police Service did not provide a completed PIIDPA Form 1.

Amherst Police Department reported under Town of Amherst. Annapolis Royal Police Department reported under Town of Annapolis Royal. Bridgewater Police Services 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. Kentville Police Service reported under Town of Kentville. Stellarton Police Department reported under Town of Stellarton. Truro Police Department reported under Town of Truro. Westville Police Department reported under Town of Westville.