PERSONAL INFORMATION INTERNATIONAL DISCLOSURE PROTECTION ACT

2016 Annual Report

Nova Scotia Department of Justice

Message from the Minister of Justice

I am pleased to provide the eleventh 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. This report is based on the PIIDPA reports received by the Policy, Planning and Research Division of the Nova Scotia Department of Justice for the period of January 1, 2016 to December 31, 2016.

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.

The Honourable Mark Furey
Attorney General and Minister of Justice

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 27, 2017, a request was sent to public bodies[1] in Nova Scotia to complete and return a *PIIDPA* Form 1 for the 2016 reporting year by March 31, 2017. 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 reminders of the requirement to report.

The 2016 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 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 three (3) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information, such as that 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 5 instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information contained in email.

2. V-LIMS (Veterinary Laboratory Information System)- See description of storage provided in the 2014 annual PIIDPA report.

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.

2. See description of conditions provided in the 2014 annual PIIDPA report.

[2] The Department of Seniors, Elections Nova Scotia, and Public Service Commission did not have access or storage outside of Canada to report.

Reasons

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

2. See description of reasons provided in the 2014 annual PIIDPA report.

Business

Description

1. Four (4) employees travelled outside Canada and may have accessed personal information via their government issued electronic devices. Traveled destinations include: United Kingdom, United States, Chile.

2. The Department of Business currently stores some boxes of files at Iron Mountain.

Conditions

1. Permission must be granted in order to take an electronic device out of county. Remote access to email is protected by username/password authentication and is delivered over a secure server. All government issued electronic devices must be password protected.

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

Reasons

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

2. The decision to use Iron Mountain was to meet the Department’s storage requirements. The Department of Business will be reviewing what is currently being stored with the hopes of significantly reducing or eliminating the number of boxes being stored at their facility.

Communications Nova Scotia

Description

1. **Google Analytics**
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. **Social Media**
   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. **Employee Travel**
   Two employees of CNS travelled to the United States with mobile devices. Two employees also had a laptop.

Conditions

1. **Google Analytics**
   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. **Social Media**
   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. **Employee Travel**
   The equipment was accessed only by Communications Nova Scotia employees.

Reasons

1. **Google Analytics**
   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**
   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. **Employee Travel**
   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. 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 'Zinio' on behalf of four regional public libraries. 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. 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.

2. Nova Scotia Provincial Library (NSPL) maintains an integrated library system (ILS) on a cost-recovery basis for a consortium consisting of 66 branch libraries in eight regional library systems, and four government department libraries. The ILS provides a library catalogue, a purchasing module, and a circulation module (check-in/check-out, and client information). The ILS is mission critical for day to day operations of libraries. Without the ILS, libraries could not function. The ILS contains personal information about identifiable individuals (library clients in Nova Scotia), including name, address, telephone number and email address. This personal information is voluntarily obtained when a client registers for a library card. Attached to the client's account number are titles currently on loan to the individual, those for which the individual has been billed and/or has paid and those which the user has requested. Transaction logs, maintained by NSPL/CCH, are retained for 3 months. The ILS is owned by an American Company, SirsiDynix, and access to personal client information from outside Canada is possible with SirsiDynix. There is no Canadian vendor which has a product suitable to the needs of a large consortia of libraries.

3. Continued use of Social Media Accounts (Twitter, Facebook, Instagram, YouTube and Flickr)

   a. Twitter: @NS_Museum, @MNH_Naturalists, @NS_MMA, @FisheriesMuseum, @RossFarmMuseum, @McCullochHouse, @Highlandv, @Sherbrooke_NS, @fundygeo, @uniackeestate, @ns_moi, @FFmuseumofNS, @SailBluenoseII, @OfficeofANSA, @NovaScotia, @GouvNE, @NS_CCHb.

   b. Facebook: Nova Scotia Museum, Museum of Natural History, Maritime Museum of the Atlantic, Fisheries Museum of the Atlantic, Ross Farm Museum, Sherbrooke Village, Highland Village Museum, Fundy Geological Museum, Museum of Industry, Perkins House Museum, Le Village Historique Acadien de Nouvelle-Ecosse, Perkins House Museum, Firefighter's Museum, Haliburton and Shand House Museums, Gus Gopher-Tortoise, Uniacke Estate , Wile Carding Mill Museum, Black Loyalist Heritage Centre, North Hills Museum, Prescott House Museum, McCulloch House Museum, Cossit House Museum, Fisherman's Life Museum, Nova Scotia Archives, African Nova Scotian Affairs, Creative Nova Scotia, Bluenose II, Acadien de la Nouvelle-Ecosse, Iomairtean na idhlig/Gaelic Affairs, Nova Scotia Provincial Libraries.

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

c. Instagram: @rossfarmmuseum, @highland_village, @firefighters_museum_of_ns, @fisheriesmuseum, @novascotiamuseum, @mnhnovascotia, @ns_mma, @uniackeestatemuseum, @blackloyalistheritagecentre, @villageacadien.

d. YouTube: Nova Scotia Museum, Highland Village Museum, Nova Scotia Archives, Nova Scotia Provincial Libraries.

e. Flickr: Nova Scotia Museums, Nova Scotia Archives, Nova Scotia Provincial Libraries. Remote access via electronic devices such as BlackBerrys, laptops, and tablets.

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

4. There were six (6) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information, such as that contained in email.

Conditions

1. Zinio had been 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. They are now investigating options related to the EU-U.S. Privacy Shield Framework. Zinio provides easy access for users to both their Privacy Policy and their Terms of Use.

2. NSPL has implemented reasonable security measures to protect personal and other information in the ILS. The ILS software is maintained at the Provincial Data Centre (PDC). 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 to strengthen privacy protection and to codify data access permissions. NSPL enables SirsiDynix to access the server for specific upgrade activities at predetermined time periods, at the end of which SirsiDynix staff are logged out by NSPL staff. NSPL staff monitor and audit to ensure the access is reasonable and appropriate. SirsiDynix has no operational requirements to access personal information about clients. Due to these precautions, the risk of access to personal information about Nova Scotians by SirsiDynix is low, but it is technologically feasible. NSPL conducted a retroactive Privacy Impact Assessment (PIA) 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. A PIA has been completed on this project. Any issues that were discovered were quickly addressed by NSPL and the appropriate regional library board.

3. N/A.

4. 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. 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. 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.

2. 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 that have products suitable to the needs of a large consortia of libraries. 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.

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

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

Community Services[4]

Description

1. Four (4) staff members travelled outside of Canada with their electronic devices in 2016. Staff member travelled to Las Vegas with iPhone from November 11-16. Staff member travelled to Japan with iPhone from September 5-21. Staff member travelled to United States with Blackberry from February 1-4. Staff member travelled to United States with Blackberry and laptop from August 31 to September 2, 2016.

2. Children in Care of the Minister of Community Services may require treatment services that are not available in the Province of Nova Scotia, and on occasion within Canada. During the 2016 calendar year, three children in care were placed in residential treatment facilities in the United States to receive residential treatment services. As part of the referral for placement to a treatment facility, information concerning the child, any medical diagnosis, treatment needs and relevant family information is shared with the placing facility. This information is provided to ensure that the facility will be able to meet the child's clinical needs and for the purpose of developing an appropriate treatment plan for the child. Information provided to the placing facility would include electronic information such as e-mails with agency social workers in Nova Scotia and paper copies of information identified above.

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

3. Since 2002, Housing Nova Scotia (formerly the Nova Scotia Housing Development Corporation) has contracted Yardi Systems, Inc. under an alternate services provider (ASP) agreement to provide Tier II application support and maintenance, as well as to manage the application hardware configuration necessary to operate the application. Tier II application support is provided by the Yardi Canadian offices operated in Mississauga, Ontario once issues reported are vetted by 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.

4. 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.

Conditions

1. Devices were password protected.

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

3. Under the terms of the contract, Yardi agrees that it will not 'use, disseminate or in any way disclose any of the confidential information' of the Nova Scotia Housing Development Corporation [Housing Nova Scotia] to 'any person, firm or business except to the extent it is necessary' to perform its obligations or exercise its rights.

4. 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.

Reasons

1. 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.

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

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

4. 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.

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, behavioral 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. Correspondence Study Program 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.

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. 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.

9. 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.

10. 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.

11. Smartsheet - Smartsheet is a software as a service (SaaS) application for collaboration and work management. It is used to assign tasks, track project progress, manage calendars, and share documents. It has a spreadsheet-like user interface, and is being used to track workflow for a major cross-department initiative.

Conditions

1. The Department of Education and Early Childhood Development has implemented reasonable security measures to protect electronic storage of personal and other information in the SIS. The information and software are maintained in a secure environment. The contract with the service provider stipulates that Department of Education and Early Childhood Development staff will authorize access to the environment to the PowerSchool Group, Folsom, 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. 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 PowerSchool Group, Folsom, California, USA stipulates that Department of Education and Early Childhood Development staff will authorize access to the environment by the PowerSchool Group technical staff for the purpose of providing periodic technical support. Staff monitor and audit to ensure the access is reasonable and appropriate. The PowerSchool Group has no operational requirement to access personal information about clients. Therefore, the risk of access to student and parents' personal information by PowerSchool Group is low, but it is technologically possible.

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

4. See above.

5. See above.

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

7. 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. 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.

9. 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.

10. 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.

11. Employees are requested to use Smartsheet for the cross-department initiative only, and not to disclose any information beyond what is required. Employees will be required to use their government email account when registering and accessing Smartsheet.

Reasons

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

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

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

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

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

6. The software is integrated with PowerSchool. Utilizing voice, SMS text and email, school administrators can send messages to parents and staff instantly and reliably. Communication with our audiences is essential, especially for school cancellations, times of emergencies, etc.

7. 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. 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 etc. are needed for preparing documents, and accessing email and Internet sites.

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

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

11. The decision to use Smartsheet was reached after an evaluation of other software solutions that do not involve the disclosure, access or storage of personal information outside Canada.

Energy

Description

1. Seven members of the Department of Energy were authorized to carry their government issued mobile phone and/or computer for personal travel outside of Canada in 11 instances in order to ensure business continuity.

2. Additionally, 19 staff travelled for business outside of Canada on 40 occasions to 10 countries and were authorized to bring their government issued mobile phone and/or computer.

Conditions

1. All devices are protected with a password and staff do not travel with or access significant personal information of Nova Scotians in their daily work.

2. See above.

Reasons

1. Staff are often required to maintain contact with the Department and continue to perform daily tasks while travelling, which requires email and other access to government records.

2. See above.

Environment

Description

1. There were 12 instances of travel in which employees travelled for work outside of Canada with a blackberry, cellphone, and/or laptop and may have accessed personal information held by the department. Travel destinations were the United States, France, Mexico, Japan, the Caribbean Islands, England, and Germany.

Conditions

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

Reasons

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

Executive Council[5]

Description

1. Seven (7) employees traveled outside of Canada on eight (8) different trips. All seven employees took their blackberries and one took a blackberry and a laptop. These employees traveled to various states in the United States of America, various islands in the Caribbean and Europe. All employees had permission from the Clerk of the Executive Council to travel with the device.

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 an 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. Four (4) employees traveled outside of Canada on five (5) different trips and took electronic devices with them. These employees traveled to destinations in the United States, Mexico, England and Japan. All employees had permission from the Deputy Minister to travel with the devices.

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

[5] In February 2016, the former Office of Planning and Priorities along with its staff became a part of the Executive Council Office and this report accounts for the activities of that Office.

(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.

Fisheries and Aquaculture

Description

1. Remote access via electronic devices such as blackberries, laptops, and tablets. There were four 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. V-LIMS (Veterinary Laboratory Information System)- See description of storage provided in the 2014 annual PIIDPA report under the "Department of Agriculture".

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.

2. See description of conditions provided in the 2014 annual PIIDPA report.

Reasons

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

2. See description of reasons provided in the 2014 annual PIIDPA report.

Health and Wellness

Description

There were no approvals granted for the storage of personal information in the custody or control of the Department of Health and Wellness outside of Canada from January 1, 2016 - December 31, 2016.

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, 2016- December 31, 2016:

1. **HealthWATCH, Shoppers Drug Mart - Drug Information System (DIS)**
The Nova Scotia Drug Information System (DIS) is integrated into the HealthWATCH pharmacy software used by Shoppers Drug Mart pharmacies in Nova Scotia to manage prescription and dispense information for customers. This integration provides a real-time data flow of

medication and devices dispensed from Shoppers Drug Mart pharmacies as required under the *Pharmacy Act* regulations. The technical support for the HealthWATCH software used by Shoppers Drug Mart is provided, in part, by resources located in Noida, India. These resources provide support for application incidents and defects, including those that would be related to the DIS integration.

The out-of-country resources providing technical support to Shoppers Drug Mart pharmacies are able to access computers in the pharmacies remotely via Virtual Network Computing (VNC). Application support is provided on a secure dedicated multi-protocol label switching (MPLS) store network that is encrypted. Support sessions are protected from “man-in-the-middle" attacks via this control. VNC sessions are initiated over a secure dedicated MPLS channel that is only used for store traffic. Technical support staff have view-only rights and cannot access DIS information until after they login with their IDs. Shoppers Drug Mart has an enterprise information security policy supported by standards, procedures and processes to protect the confidentiality, integrity and privacy of PHI data.

A Request for Approval to Access and/or Store or Back-up Persona/Information Outside Canada Pursuant the Personal Information International Disclosure Protection Act (PIIDPA) was submitted in July 2016 to permit the above access to personal information contained within the DIS.

2. **Panorama, IBM Canada Ltd**
   IBM Canada Ltd. provides the proprietary software called Panorama for use by Public Health within Nova Scotia through a cloud based Managed Service. Panorama is an electronic application that will enable Nova Scotia to effectively collect key public health information. Technical support for the software is provided, in part, by resources located outside of Canada. All personal health information will be stored in Canada using IBM's Canadian Cloud Service called "SoftLayer" located in Toronto, Ontario, with a second (Disaster Recovery) site in Montreal, Quebec. No data will be stored outside Canada. All data in transit will be protected via encryption (Hypertext Transfer Protocol, HTTP, within a connection encrypted by Transport Layer Security). Access by out-of-country resources will be via IBM's secure private network. The administrative virtual private network (VPN) will enable IBM to administer and manage the devices ordered and to upload, download, and manage content.

   The *Request for Approval to Access and/or Store or Back-up Persona/Information Outside Canada Pursuant the Personal Information International Disclosure Protection Act (PIIDPA)* was approved in December 2016 for this project.

3. **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. The resources only had access to view the data and could not update nor change the data. Access was critical to meet the timelines of the project and limited to a period from March 8, 2016 until July 31, 2016.

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, 2016- December 31, 2016:

4. **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 in any one of several 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.

5. **McKesson Corporation, Relay Health - HealthLink 811**
   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.

6. **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.

7. **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 Nova Scotia Health Authority Privacy Leads and other appropriate NSHA/IWK/Department of Health and Wellness staff using the application and audit log data.

8. **DHW Employee Access**
   Between January 1, 2016 to December 31, 2016, two (2) 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).

Removed:

9. **McKesson Corporation, Relay Health solution: Personal Health Record (PHR) Pilot Project**
   Further assessment on the McKesson Relay Health (MyHealthNS) access needs has determined that support services for MyHealthNS data are delivered in Canada. If there is a need for on-time, specialized support skills that cannot be delivered in Canada, a specific PIIDPA request for the event will be issued and approved as and when needed.

Conditions

1. **HealthWATCH, Shoppers Drug Mart - Drug Information System (DIS)**
   The Master Services Agreement between Shoppers Drug Mart and the out-of-country technical support vendor includes provisions to protect confidential information, which includes all information transmitted in any form by Shoppers Drug Mart stores and customers. The contract specifies that the vendor must maintain confidential information in strict confidence, and may not disclose the information without prior written consent of the disclosing party.

   Shoppers Drug Mart signed a *Confirmation of Acceptance and Drug Information* System *Confidentiality Agreement* as detailed in the *DIS Joint Service and* Access *Policy (Pharmacy Software Vendors).* This policy states that "Pharmacy Software Vendors shall not access the DIS from outside Canada or transfer information from the DIS to locations/computer systems/networks outside of Canada unless prior written approval has been received from the Province." The policy also details the responsibilities of Shoppers Drug Mart as the software vendor to ensure that collection, use, and disclosure of personal health information within the DIS will be in accordance with the *Personal Health Information Act* (PHIA).

2. **Panorama, IBM Canada Ltd**
   Data will be stored in data centres within Canada.

   The Master Services Agreement between IBM and the Province (DHW and ISD) includes Schedule 15 Privacy and Security Obligations which defines the conditions under which access is provided for out-of-country technical support.

   Provisions of the Agreement cover Non-Disclosure of Personal Information and Personal Health Information, Ownership and Control of Provincial Data, Privacy and Security Training, Security and Privacy Related Certifications, Assessments and Reports, Limiting Access to Authorized Personnel, a Confidentiality Covenant for Personnel, and Non-Compliance Reports. The Agreement includes vendor provisions to protect confidential information. The vendor must maintain confidential information in strict confidence and may not disclose the information without prior written consent of the disclosing party. The Agreement details the responsibilities of IBM as the vendor to ensure that collection, use, and disclosure of personal health information will be in accordance with *PHIA.*

   From a Managed Service perspective, protections are put in place where, should administrative rights be required to perform Level 2 support, permission will be granted by IBM Canada to provide temporary administration rights, long enough to perform any work related directly to the Level 2 support issue. In some cases, this support will be handled by the Global IBM support team. All access to any Provincial data files (including personal health information) is logged, and audited by IBM to ensure no inappropriate actions are taken by any member of the Level 2 support team. The Province has the right to review any logs and audit material.

3. **SAP Enablement for DHA Transition project**
   CGI Global team resources were limited to view only and not in possession of the 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.

4. **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.

5. **McKesson Corporation, Relay Health - HealthLink 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.

6. **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 is 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 in the NSHA IM/IT data center. All users accessing the data will require security sign-on and will need to be given access by the hospital IT staff.

   Select McKesson developers/testers will have access to the test system. McKesson developers/testers will be pre-approved and must sign a confidentiality agreement. McKesson developer's/testers access will be terminated immediately at test completion. No personal information will be downloaded or copied by McKesson. All requests into SHARE is tracked, and audit reports may be provided for review.

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

7. **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 NSHA IM/IT when they access the server to perform maintenance. Access logs will be reviewed for compliance. No patient data will be downloaded or copied from the appliance.

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

8. **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. **HealthWATCH. Shoppers Drug Mart - Drug Information System (DIS)**
While there are other pharmacy software applications in the Canadian market, the choice of software is determined by pharmacy organizations. Shoppers Drug Mart's HealthWATCH software is an in-house application that is unique to Shoppers Drug Mart and not used by other pharmacies in Canada. For pharmacies to meet their legal obligations to connect to the DIS under the *Registration, Licensing and Professional Accountability Regulations of the Pharmacy Act;* all software vendors in Nova Scotia must integrate with the DIS. Providing technical support for the software is necessary for business continuity for Shoppers Drug Mart pharmacies in Nova Scotia.

2. **Panorama, IBM Canada Ltd**
Panorama will enable the DHW Public Health program to fulfill its mandate, under the *Health Protection Act,* in the prevention and containment of disease through the provision of high quality, timely health surveillance data at the regional, provincial/territorial and Pan-Canadian levels and related public health data at the regional and provincial levels.

   Panorama provides a proven Pan-Canadian public health solution that is currently used by six different jurisdictions across Canada, offering Nova Scotia a modern public health solution where one does not currently exist.

   The intended scope of the Panorama Implementation Project includes Vaccine Inventory, Immunization, and Communicable Disease Investigation and Outbreak Management.

3. **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 nondisclosure/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.

4. **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.

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

6. **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.

7. **FairWarning**
   The FairWarning application will be used to augment current user access audit approaches for various provincial health information systems. FairWarning is an appliance based application that facilitates the creation of privacy audit reports for health information systems. The FairWarning tool allows audits to be conducted of user access to electronic health information systems. The application will be used to augment current user access audit approaches for various provincial health information systems.

8. **DHW Employee Access**
   When staff is traveling for business reasons (e.g. meetings, conferences) they are expected to monitor their e-mail and voice mail where possible. Therefore, it is necessary for them to check e-mail remotely where possible 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 BlackBerrvs, laptops, and tablets. There were seven (7) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information, such as that 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 CSSL) 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. **Travel outside of Canada with Electronic Devices**
   Thirty (30) employees accessed their government email while travelling outside of Canada, to the United States, on business 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) business trips outside of the country in 2016 in which they accessed government email while out of the country.

2. **Pictometry Connect Explorer**
   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. **SAP Ariba**
   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.

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

5. **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 change in personal information access or storage outside Canada since the 2013 Finance and Treasury Board 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.

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

7. **Operational Accounting**
   The Royal Bank of Canada (RBC) contract awarded in 2010 by the Province of Nova Scotia to provide electronic vendor payments to US vendors/individuals for the period of February 2013 to January 2016 was extended to March 2021.

Conditions

1. **Travel outside of Canada with Electronic Devices**
   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. **Pictometry Connect Explorer**
   This information is subject to the Pictometry Privacy Policy.

3. **SAP Ariba**
   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. 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.

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

5. **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.

6. **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.

7. **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 vendors.

<u>Reasons</u>

1. **Travel outside of Canada with Electronic Devices**
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. **Pictometry Connect Explorer**
This allows the province to access oblique photographs to align with Municipal Partners.

3. **SAP Ariba**
The SAP Ariba Service is not available in Canada.

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

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

5. **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.

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

7. **Operational Accounting**
Electronic vendor payments provide a low cost, flexible and highly reliable payment system to vendors.

   The requirement to electronically forward funds to vendors located in the U.S. requires that information flows through an Automated Clearing House (ACH).

   There is no ACH that stores information in Canada.

Justice[6]

Description

1. **Staff Travel**
Seventeen (17) employees traveled outside of country with a Blackberry or laptop that contained personal information or could access personal information.

2. **Correctional Services**
In 2008, Correctional Services awarded JEMTEM Inc. the contract for Electronic Supervision of Offenders.

3. **Legal Services**
Legal Services uses 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. **Court Services**
The Director of the Maintenance Enforcement Program 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. **Policy and Information Management**
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.

[6] Report includes the Medical Examiner's Service, and the Serious Incident Response Team (SIRT).

Conditions

1. **Staff Travel**
   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. **Correctional Services**
   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. **Legal Services**
   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. **Court Services**
   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.

5. **Policy and Information Management**
   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.

Reasons

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

2. **Correctional Services**
   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. **Legal Services**
   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. **Court Services**
   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.

5. **Policy and Information Management**
   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.

Labour and Advanced Education

Description

1. 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 GED® is composed of a series of five tests that evaluates participants' skills and knowledge in the areas of Language Arts-Reading, Language Arts-Writing, Mathematics, Social Studies, and Science. The GED® is an internationally recognized assessment tool of high school equivalency. The GED® credential is accepted by employers across Nova Scotia and Canada, and serves an important function for labour mobility.

   The GED® tests are designed to measure the skills that correspond to those of recent high school graduates. The tests involve the ability to understand and apply information; to evaluate, analyze, and draw conclusions; and to express ideas and opinions in writing. Adults who pass the five tests receive a Nova Scotia High School Equivalency certificate of Grade 12. There are approximately 1,500 tests conducted each year in Nova Scotia. The department scans the test sheets locally and sends data to NRSPro over an encrypted Secure Sockets Layer (SSL) connection. The information is stored in a database at NRSPro located in Spanish Fork, Utah, USA, for processing and as a record for future reference. Continued storage is required for data retrieval and combining of score results for students re-writing tests that were not passed successfully. In the event the department terminates services with NRSPro the data will be returned/transferred to the department or another service provider and removed from the NRSPro database.

   The test scoring is completed remotely by NRSPro and the test results and certificates are transmitted to the department in PDF files for printing locally. The transmission is over a SSL connection using an encrypted link. The test results and certificates are also available for viewing by authorized LAE staff on the NRSPro website, using the same security methods. A user ID and password is also required for access. In addition, the information is transferred by NRSPro to the General Educational Development Testing Services (GEDTS) international database.

   The international database contains information used for statistical reporting of GED achievements by jurisdiction. This includes gender, age, country, province, number of participants, number/percentage passed, and number/percentage failed. The international database is housed by Marsys a service provider located in Miami, Florida, with a backup database maintained at their office in San Mateo, California. Marsys have a contract with GEDTS for support and management of the GEDTS international database. The international database was established in support of the GED program and it is mandatory that jurisdictions agree to send data to GEDTS as part of the GED licensing agreement.

   The GED Testing Service (www.GEDtest.org) is a program of the American Council on Education (ACE) which develops, delivers, and safeguards the GED Test, setting the policy for and ensuring compliance of test administration. GED testing is administered by each of the 50 states and the District of Columbia, the Canadian provinces and territories, the U.S. insular areas, U.S. military and federal correctional institutions. On March 15, 2011, ACE in partnership with Pearson announced the creation of a new business, GED LLC to design, develop and deliver a new GED test. The new GED Testing Service is to be based in Washington, D.C. with additional offices in Minneapolis, Minnesota.

2. 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.

Conditions

1. The department has a contract with NRSPro which stipulates that all information will be kept private and confidential and will not be released to 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.

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

Reasons

1. The department completed an evaluation of options for delivery of the Nova Scotia GED program in November of 2001. It was determined that there were only two vendors (OSS & NRSPro) certified by GEDTS to conduct test scoring that the department felt confident would be able to handle Canadian requirements. Both vendors were application service providers (ASPs) located in the USA. The ASP model included storage of the data at a vendor location in the USA. At the present time, there is no option of a software solution with data storage in Canada. The other option available to the department in 2001 was to custom develop a system to manage the GED program, and then apply for certification as a testing facility with GEDTS. This option was not chosen due to cost and time constraints to conform with GEDTS program changes in 2002. This would have resulted in an interruption in client service to allow time to design the system and obtain certification from GEDTS.

   In 2001, the department's decision was made to contract with OSS (Oklahoma Scoring Service) based in Norman, Oklahoma, USA for the 2002 GED test series, based on their extensive experience in GED test scoring, maturity of the software solution, security methods in use for transmission of information, and high reputation across educational jurisdictions. In addition, OSS came highly recommended by GEDTS.

   In July 2009, the department terminated our contract with OSS and began working with NRSPro.com. Data was transferred to our new service provider, NRSPro. NRSPro had been the department's scoring service provider from 1993 to 2001, prior to the release of the 2002 test series and the new technical scoring requirements (uploads to the IDB).

   The decision to switch to NRSPro came from polling other Canadian provinces. It was determined that NRSPro provided an overall better service, including instant scoring and immediate reporting times, detailed reports, incorporating NS forms and letters as report options and allowing students and third-party verifiers to get instant results online.

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

Municipal Affairs

Description

1. Nine (9) 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 SSL encrypted link.

Reasons

1. Allowing staff to have 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 15 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. Nine (9) employees traveled outside of Canada on 22 different trips. All nine employees took their blackberries and one took a blackberry and an iPad. The employees traveled to various states in the United States of America, Aruba, and Europe. Two (2) employees travelled to Hong Kong, China, South Korea and Japan. In this instance, burner phones were provided from Intergovernmental Affairs. All nine employees had permission from the Chief of Staff, Office of the Premier to travel with the device.

Conditions

1. Two (2) employees travelled to Hong Kong, China, South Korea and Japan. In this instance, burner phones were provided from Intergovernmental Affairs.

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 eleven (11) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information, such as that 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.

Public Prosecution Service

Description

There was no storage of personal information outside Canada by the Public Prosecution Service.

1. There was access to personal information using wireless data devices including Blackberry and laptops by 11 individuals 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.

Tourism Nova Scotia

Description

1. Remote access via electronic devices such as blackberries, laptops, and tablets. There were 16 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 Mail Chimp. See description in 2013 Annual PIIDPA report.

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.

2. MailChimp, see conditions provided in the 2013 annual PIIDPA report.

Reasons

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

2. MailChimp — see description of reasons provided in the 2013 annual PIIDPA report.

Transportation and Infrastructure Renewal

Description

1. There were thirty-two (32) 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 2016. Three travelled to Europe, two to the Caribbean, one to the United Kingdom and twenty-six (26) to United States.

   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 allow employees 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 2013/14, 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[7]

Description

1. SNS currently stores approximately 25,000 boxes of records with Iron Mountain. While the records are stored at a facility in Nova Scotia, Iron Mountain is a U.S.-based company and the database maintained by Iron Mountain is accessible in the United States.

2. Eight (8) SNS staff traveled outside Canada during the reporting period on thirteen (13) separate occasions. One staff member travelled six times. SNS staff took their laptop and/or mobile device phone with them while out of the country.

3. In 2006, Morpho Trust USA (formerly L-1 Identity Solutions) (formerly Digimarc) of Billerica, Massachusetts was awarded a contract to provide Photo License/Photo ID equipment, software integration, and support services to the Registry of Motor Vehicles. This contract included a major upgrade to the Photo License/ID Card system in 2010. The Photo License image/database server (a key component of the system which stores client photos, digitized signatures, personal information, and Driver Master Number) is located at the Provincial Data Center in Halifax, Nova Scotia. In 2006 and continuing, Digimarc support technicians in Billerica, Massachusetts and Fort Wayne, Indiana have been provided remote access via VPN to the image/database server in order to provide tier II/III support. Routine maintenance and support for this system is provided by Halifax-based Morpho Trust 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.

4. SNS uses a Google Analytics service to monitor several of the public facing services it delivers on behalf of government. Information about a user's interaction with these services is sent to Google servers (located primarily in the United States) where analytics are performed and statistical reports are created and made available to the Province. The only information disclosed to Google that could be considered personal information is the originating IP address.

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

Conditions

1. Iron Mountain is under contract to maintain safe and private storage of SNS records. The Iron Mountain database does not include personal information; only box number information.

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

3. 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.

4. To minimize the privacy risks associated with the use of the IP address by Google, the anonymization feature was employed. This means the IP address is masked by setting the last digit in the IP address octet to zero. This process occurs after the IP address is disclosed to Google. Therefore, it is possible that the IP address could be accessed by Google prior to performing the anonymization process. Google has indicated that the full IP address will not be stored on its servers which is consistent with their privacy policy.

Reasons

1. The Provincial Records Centre used to store their records overflow at Iron Mountain until the mid to late 1990s. In 1997, the Iron Mountain accounts created by the Provincial Records Centre were transferred to the various departments who had overflow records stored with Iron Mountain. At that time, SNS took over ownership of the Iron Mountain relationship.

   Service Nova Scotia also had records stored at Canadian-based Securit Records Management. In 2014, Iron Mountain acquired Securit transitioning additional SNS records to Iron Mountain.

   The Provincial Records Centre will not currently accept any records from SNS that are not covered by an approved records classification and retention schedule following the provincial standard (STOR). Until SNS develops STOR and finds the funding to transfer the records out of Iron Mountain, SNS has no alternative but to continue to use commercial storage facilities. No viable Canadian options exist.

2. Maintain contact with operations.

3. Access by Morpho Trust USA (formerly L-11dentity 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.

4. Analytics provide insight into user behaviours and support evidence based decision making related to investments in on-going system improvements. It is an essential tool in SNS's continual improvement approach to developing digital services and supports the responsible fiscal management of public resources.

Foreign Access and Storage by Agencies, Boards & Commissions and Other Public Bodies[8, 9]

Atlantic Lottery Corporation

Description

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

2. Travel with electronic devices: A number of AL staff traveled outside Canada and have the ability to access personal information contained in email or stored in the Microsoft Office 365 system, using devices including cell phones, iPads, BlackBerrys and laptops. AL staff seek authorization prior to taking devices across the Canadian border.

Conditions

1. E-mail, storage and collaboration:

    a. Employee's access to content is restricted through secure authentication over an encrypted connection.

    b. Office 365 services follow industry cryptographic standards such as TLS/SSL and AES to protect the confidentiality and integrity of its customer data.

        i. For data in transit, all customer-facing servers negotiate a secure session by using TLS/SSL with client machines to secure the customer data. This applies to protocols on any device used by clients, such as Skype for Business Online, Outlook, and Outlook on the web.

        ii. For data at rest, Office 365 deploys Bit Locker with AES 256-bit encryption on servers that hold all messaging data, including email and IM conversations, as well as content stored in Share Point Online and One Drive for Business. BitLocker volume encryption addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers and disks.

    c. In the case of Office 365, AL promotes the use of Office 365 as a secure, industry-standard solution. The company provides information on the protection of privacy and

[8] The Human Rights Commission, Nova Scotia Public Service LTD Plan, Office of the Police Complaints Commissioner, Divert NS (Resource Recovery Fund Board Nova Scotia or RRFB Nova Scotia), the Nova Scotia Provincial Lotteries and Casino Corporation, and Workers' Compensation Appeals Tribunal did not have access or storage outside of Canada to report.

[9] The Council on African-Canadian Education did not provide a completed PIIDPA Form 1.

encourages employees to avoid storing or communicating private information unless it is necessary to the performance of their job.

   d. AL is currently working with Microsoft to transition its content and services to the newly opened Canadian Datacenters.

2. Travel with electronic devices:

   a. See the above restrictions or conditions for E-mail, storage and collaboration.

Reasons

1. Cloud based e-mail, storage and collaboration software is now industry-standard.

2. 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.

Halifax Harbour Bridges[10]

Description

1. HHB's MACPASS software application maintenance and support is provided by BriC primarily located in Irvine California. BRiC provides both routine maintenance and upgrades 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 employees require written permission authorized by the CEO to take devices outside of the country.

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 is there is an issue that needs to be communicated). HHB also uses the account to share photos and short videos and other communications we want to share with the public. The public use Twitter to communicate directly with us as well with their questions and comments. The second account is @BigliftHFX and is used to communicate the status of the Big Lift project.

[10] Formerly operated as Halifax-Dartmouth Bridge Commission.

Conditions

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

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 Complian, SSAE-16 compliant (formerly SAS70), and full-strength encryption and central administrative control (web and mobile). All web data transmitted to/from BoardBookit applications is TLS/SSL encrypted. Permissions and access within BoardBookit are tied to individual users administered by HHB.

3. 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 HHB's network connect over a virtual private network that uses dual layer authentication (domain authentication and a token).

4. HHB uses Twitter to share information and interact online with the public and organizations in 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.

Reasons

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

2. Limited availability for an equivalent 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 12 instances of employees travelling for business or work with their laptop or other electronic devices.

4. Social media platforms are used to engage the community, increase public awareness and to promote the dissemination of accurate, timely information. Other social media sites HHB uses includes: Facebook, Instragram and You Tube. HHB does not collect any personal information on these sites.

Innovacorp

Description

1. DealFlow -Sevanta Systems provides software and workflow consulting services to venture firms, private equity groups, and Fortune 500 corporate investment teams through the world. Launched in 2005, Sevanta Dealflow, was designed as a full-service, customizable dealflow management solution based on our deep experience in the field. Sevanta Systems Corporation is a U.S. corporation headquartered in Miami, Florida, Pursuant to s. 5(2) PIIDPA, the head of Innovacorp 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 is to meet the necessary requirements of Innovacorp's operation.

2. SurveyMonkey: Innovacorp utilized SurveyMonkey a total of 3 different times during 2016. SurveyMonkey is an online survey development cloud-based software, and as a service company, was 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.

   SurveyMonkey's email campaign management services was used for storage and access of anonymous employee survey data. Pursuant to s. 5(2) PIIDPA, the head of Innovacorp 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 operations.

3. Innovacorp employees accessed information internationally a total of 19 different times during 2016. Pursuant to s. 5(2) PIIDPA, the head of Innovacorp 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. DealFIow - Data services, including storage, access, and 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.

   SurveyMonkey's e-mail campaign management services: The storage and access of anonymous employee survey data is to be protected in accordance with the SurveyMonkey's terms of service.

3. 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 the Innovacorp's Code of Conduct and Innovacorp Information Technology Policy.

Reasons

1. DealFlow - Services including storage, access, and client/partner/service provider representatives' personal information (primarily business information): Innovacorp requires a robust and secure platform to store and manage information necessary for the conduct of Innovacorp's relationships with its clients, prospective clients, partners and stakeholders. The DealFlow 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 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.

   SurveyMonkey's email campaign management services: Domestic suppliers currently do not meet Innovacorp's technical and service requirements.

3. 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 traveling outside Canada.

Nova Scotia Business Inc.

Description

1. Salesforce.com, Inc. 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. 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. There were 43 employees who were approved to access their wireless devices (e.g., cell phones/BlackBerrys/iPhones/iPads/laptops) while travelling outside Canada for business and personal reasons for a total of 130 trips taken in 2016.

3. VerticalResponse, Inc. 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 email campaign management services supplied under contract by VerticalResponse, Inc. (a US corporation with its principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.

4. Proposify (PitchPerfect Software, Inc.) is a sales proposal management services, storage and access of 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 and investment attraction services. 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.

Conditions

1. Salesforce.com, Inc. 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. 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.

3. VerticalResponse, Inc. 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.

4. Proposify (PitchPerfect Software, Inc.) The individuals' business contact information (name, email 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. The personal information (primarily business contact information) is to be protected in accordance with the service agreement including confidentiality provisions.

Reasons

1. Salesforce.com, Inc. 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. 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.

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

4. Proposify (PitchPerfect Software, Inc.) 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. 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.

Nova Scotia Health Research Foundation

Description

1. Three instances in which employees of the Nova Scotia Health Research Foundation travelled outside of Canada for business or personal trips with their cell phone and/or laptop.

Conditions

1. The employees were expected to maintain communication with, or be reachable by, staff at the office. The devices are password protected.

Reasons

1. When staff travel, they may be required to conduct business or maintain contact with the office. Appropriate approval was obtained.

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 Liquor Corporation

Description

1. Sixteen (16) NSLC employees travelled outside of Canada on business with their personal devices in 2016. Travel destinations included: US - New Orleans, Louisiana, Chicago, Illinois, Scottsdale, Arizona, Las Vegas Nevada, Orlando, Florida, Hoboken, New York, Denver Colorado, Boston, Massachusetts, Atlanta & Hickory, Georgia and San Francisco, California; London, United Kingdom; and Dusseldorf, Germany.

Conditions

1. Password protection on all NSLC devices for access to email via the portal or webmail. For access on a laptop, login credentials are required. This is for access only, there was no storage.

Reasons

1. This is necessary to maintain daily business operations.

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 and related human resources records. Ceridian Canada is a subsidiary of Ceridian HCM Holding Inc., a US company.

2. Employee Access to Personal Information by Mobile Device:

- **Employee Access to Personal Information by Mobile Device (Blackberry or Computer)**. There were five instances of employees traveling 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. Mobile devices have encrypted storage to protect personal information that may be saved locally.

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

Reasons

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

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.

2. The online survey program used by Trade Centre Limited is hosted out of San Mateo, California, USA. The data is housed with Survey Monkey Inc. (and its subsidiary company, Infinity Box Inc.) in SOC 2 accredited data centres which are certified and compliant with the EU-U.S. Privacy Shield Framework. Survey Monkey is also PCI 3.1 and HIPAA compliant.

   The survey data collected is for internal training surveys and customer satisfaction surveys. All survey data collected is owned by 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) (c)ustomer 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.

2. Two members of the TCL staff have access to the online survey program. Access to the survey program requires authentication by way of unique usernames and passwords which are stored in an encrypted format.

   Any personal data which includes email addresses, first and last names of clients, or TCL staff members, is owned by TCL and used only to collect feedback for the purposes of HR training and client satisfaction surveys. Email addresses used to invite survey participants are safeguarded and only available for TCL use.

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, 2018.

   Legal counsel was sought on the original agreement in regard to best practices and privacy requirements; the contract was found to be sound.

2. During 2016, TCL sought out online survey programs that would host data within Canada. However, with the sale of Fluid Surveys to Survey Monkey, it was suggested that Survey Monkey would best meet the needs of our organization at this time.

Waterfront Development

Description

1. There were instances when staff travelled outside Canada and brought Waterfront Development owned devices such as iPhones and/or laptops with them. These devices are configured to check for email, the contents of which may have contained personal information.

Conditions

1. Remote access to email is protected by username/password authentication, and encrypted using industry standard TLS/SSL encryption. All iPhones and laptops are required to be password protected and all iPhones are fully encrypted.

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.

Workers' Compensation Board of Nova Scotia

Description

1. Employee access to personal information by mobile device (iPhone, iPad, Blackberry) or computer (laptop, desktop) - 49 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. Translation Services - 11 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. Language interpreters may be located outside of Canada. Calls are not recorded or documented therefore no information is collected or stored outside of Canada.

3. Employee access to personal information by remote access - 65 individual's personal information (contained in unique claim files) accessed from a remote location outside of Canada (in the US) through a secure portal into the WCB's internal network by remote access.

4. Medical Consultant access to personal information - 44 instances of access to personal information (contained in unique claim files) accessed from a remote location outside of Canada (in the US) through a secure portal into the WCB's internal network by remote access.

Conditions

1. Access to WCB's internal network is protected by username/password authentication, and is delivered over a secure portal based on accepted industry practices.

2. Language Line obtains a signed confidentiality agreement from each respective interpreter and reviews these agreements annually. The interpreter service is provided over the phone and does not result in downloading, printing or documentation of any personal information or elements of the call. 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 only after the WCB obtains the consent from the individual.

3. Immediate reporting of theft/loss of any device or information is required in all associated contracts.

4. All such access is governed by agreements with appropriate privacy and access requirements. Information shared is limited to only necessary medical information required to complete a review and provide medical reports.

Reasons

1. When WCB 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 on this access as noted above.

2. The third party language 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 only over the phone.

3. N/A

4. The out of country medical consultant specializes in both occupational and environmental medicine, providing unique capabilities. The service of this consultant is required in the interest of allowing the WCB to administer the *Workers' Compensation Act*, Regulations and Policy.

Foreign Access and Storage by District Health Authorities and Provincial Health Care

Nova Scotia Health Authority

Description

1. As noted in past reports, vendors requiring access to personal information from outside of Canada are granted access on a need to know basis for NSHA operations, or when expertise does not exist, or is not available in Canada. Agreements and contracts with vendors are in place, and NSHA IT facilitates access as needed.

2. Mobile device use: For 2016, NSHA reviewed phone records, which indicate 622 instances where mobile devices (i.e. Blackberry) were used outside of Canada where personal information or company e-mail may have been accessed.

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. NSHA privacy policies also apply. Program areas/vendors must make case as to why a PIIDPA exception is required, and approval must come from CEO.

   All Privacy Impact Assessments focus on PIIDPA, on whether or not information will be accessed or stored outside of Canada, and what mitigations are in place (e.g. process for informing remote access will occur for service reasons/limiting personal information present).

   Staff are directed towards in house solutions when one exists, rather than using web-based cloud services. Authorization from the Privacy Office based on need is required in these cases.

2. 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 PIIPDA is complied with.

2. Staff members may be granted approval to access personal information when travelling for patient care, business continuity, and operational support. Using an NSHA supported device is seen as a more secure method than staff relying on other less-secure methods.

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 2016 calendar year, IWK worked with **90** American laboratories, **51** international and **50** 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:
   - Meditech: Boston, Massachusetts, USA (IWK patient information system);
   - GE Healthcare: United Kingdom (ultrasound system); and
   - USA Phillips (Obstertical Trace View , Ecelera system Cardiology).

3. **Business Travel:**
   IWK's records indicate that during the 2016 calendar year, there were approximately **96** incidents of travel booked through the IWK for work-related travel outside of Canada, by **82** 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, and are not typically used to transport or access personal information.

Conditions

1. **Laboratory Testing**
   Consent is obtained from patients wherever practicable prior to sending samples to referral laboratories outside of Canada. IWK refers specimens to genetic referral laboratories in accordance with guidelines established by the American College of Medical Genetics (AMCG) and Canadian College of Medical Geneticists (CCMG). Further, IWK refers to laboratories that meet conditions of international and national regulatory organizations, including International Standard ISO 15189, Medical Laboratories – Particular Requirements for Quality and Competence. ISO 15189 addresses the selection, assessment and monitoring of the referral laboratories and confidentiality requirements. Laboratories that do not meet these conditions may be used at the discretion of the clinician and care team if deemed appropriate and necessary. All referrals are tracked by two laboratory information systems, (LIS) Meditech and Shire Management System (SMS). Any new IT/electronic medium used to facilitate referral services has a Privacy Impact Assessment completed prior to use.

2. **Non-Canadian Contractors/Vendors with Remote Access**
When IWK contracts with service providers where there is potential for storage of or access to personal information outside Canada, wherever practicable, IWK obtains individuals' consents or uses contractual conditions to protect privacy and confidentiality (including requiring vendors to agree to secure network access requirements, confidentiality clauses, and other accountability measures intended to safeguard personal information). When dealing with large vendors, Site-to-Site VPN access can be used.

   IWK's Department of Biomedical Engineering scrubs/destroys all personal information stored on equipment when sent outside the Health Centre for repair or servicing.

   IWK's Privacy Office has implemented a process for approvals of remote access given to vendors, supported/executed by IT, 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 Coordinator 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 to maintain the visibility of traffic and the enforcement of security policy for protection against known and unknown threats. IWK laptops and 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:

   - "Active Directory" software protections are in place for Terminal Servers and Remote Desktop Stations, which allows IWK network administrators to control what users can do when accessing the IWK network remotely. Certain functions are controlled or prevented, e.g.: copy/paste, remote printing and mapping of serial and printer ports. This software turns a remote access session into a "window" capable of viewing IWK systems, but prevents information from being removed from the system.
   - IWK 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.

- IWK laptops use encryption software to safeguard information stored on any lost, stolen or improperly accessed laptops, including USB portable memory drives used in those laptops. Reported lost or stolen devices can be selectively wiped to ensure that corporate data on the device is not compromised.

Reasons

1. **Laboratory Testing**
   Obtaining certain specialized laboratory testing services from outside Canada is necessary for IWK's operations. Genetic testing is an evolving field continually requiring increasingly esoteric testing. IWK provides genetic testing for the Maritime Provinces, and required testing sometimes is cost prohibitive to obtain in Canada or is not available in Canada at all, necessitating international referrals.

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

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

Foreign Access and Storage by Universities and Colleges[11]

Acadia University

Description

1. **Business Travel.** Acadia staff and faculty participated in 72 international trips in 2016. Employees have access to their email via smart phone, tablet, or laptop. All Acadia employees also have access to Office 365 resources such as mail, SharePoint and OneDrive.

2. **Office 365.** Acadia staff, faculty and alumni all have access to Office 365 resources which includes online OneDrive, SharePoint, mail, contacts, and calendar. These resources are used for everyday business work, collaboration and data storage. Web access is available to sites for authorized users. Data Storage is in a US data centre.

3. **Advancement Event Management.** Acadia University Advancement - Alumni Affairs uses Attend.com to organize, distribute and obtain information about alumni events. Attendees can sign up for events through the system (capturing name, email and payment information). These are provided by Alumni registering for an event. Alumni may use mobile device, tablet or laptop/desktop to access attend.com. Events are organized on a semi-regular basis based on the schedule as set by Alumni Affairs. Data is stored in Boston, MA, USA. Data is accessed internationally as Acadia has international Alumni and events are held in cities around the world.

4. **Alumni/Donor Information.** Divinity College uses their own alumni/donor database software provided by an American vendor, Blackbaud. Alumni and donor data is hosted by a vendor on a Canadian cloud system. The data centre is in Vancouver. The vendor provides technical service from time to time via remote access while under the supervision of Divinity personnel.

5. **Learning Management System.** Acadia uses Moodle as its learning management system. The system facilitates online learning for both on-campus students and those studying from a distance. It is used by Open Acadia and the Acadia Divinity College. Web access is available to this system for both faculty delivering courses and students enrolled in the courses. The students enrolled in the courses may be on campus or from international locations.

6. **Ticket Management System**. Acadia University - Technology Services implemented Team Dynamix as its IT Service Management & Project Management Software. It is stored within Acadia's own data centre.

7. **Enterprise System**. Colleague is an Enterprise system that contains employee, alumni, donor information. Both on and off-campus access is controlled through authorized credentials. Off campus access to TSONLINE, a web component to Colleague that provides access to time reporting and payroll information, requires 2 levels of authenticated credentials -via VPN and then within the site. Advancement Staff, who travel to various international locations, access and enter information regarding donors/alumni while traveling. There are alumni 'Life Officers' who run Alumni events in international locations. They receive lists of local alumni via an Acadia SharePoint site. Further safeguards are in place so that Alumni may only access the data related to their location.

[11] Atlantic School of Theology did not have access or storage outside of Canada to report.

8. **Communication**. Constant Contact is an email marketing software. Names and email addresses are stored within Constant Contact. It is used at Acadia University to communicate with Alumni and donors, many of whom live internationally. The information is uploaded from the Acadia database. Alumni/Donors can unsubscribe/opt out of the email messages.

9. **Recruitment**. eZRecruit is a web-based platform designed to help educational institutions recruit students and manage relationships with institutional stakeholders. The system is integrated with Acadia's Student Information System. The Acadia Student Information System is stored in an on-campus, Acadia datacentre. eZRecruit is a cloud based with datacentres in the US. Acadia Recruitment officers require access while on the road. Applicants may reside in international locations.

Conditions

1. When accessing outside of Canada, staff are using work related laptops/mobile devices that are password protected and authenticated login credentials. Alumni access through authenticated Acadia SharePoint sites. Life Officers are required to sign a privacy/confidentiality agreement with the Office of Advancement outlining the use and destruction of the data.

2. To access the Office 365 portal, users must have an Acadia authenticated credentials and data stored within the Office 365 site is encrypted and secure. For access to additional programs on campus, access is acquired through the VPN with authenticated logins/passwords. Data at this point is protected within the firewall. To access the Office 365 portal, users must have Acadia authenticated credentials. Data stored within the Office 365 site is encrypted and secure. For access to additional programs on campus, access is allowed through the VPN with authenticated credentials. Data at this point is protected within the firewall.

3. Access to Attend.com by Acadia staff is limited to those who are required to use it for their work. It is a password protected login that requires authentication from the Attend.com server. As it is a web-based product, it can be accessed from within Acadia or when staff are on the road at the events. This access could be international.

4. Limited access where required for maintenance and troubleshooting. Contractual security measures including restrictions on access to and disclosure of information by service provider and employees (https://www.eventfarm.com/privacy-policy).

5. Storage of data is housed within the Acadia University data centre. Access to the data is via appropriate login credentials and only authorized individuals can access data.

6. Access to personal information from outside of Canada is limited to authorized personnel, with authenticated logins.

7. The source of support for Colleague is in Canada. However, in the case of an external entity requiring access for troubleshooting an issue, all access is controlled, recorded (via BomGar software), and done under the supervision of Acadia Staff. Access to personal information (name, email address, work contact information) is limited to authorized personnel. In the case of an external entity requiring access for troubleshooting an issue, all access is controlled, recorded (via BomGar software), and done under the supervision of Acadia staff.

8. Constant Contact provides policies regarding the safekeeping with respect data storage and security: physical, network, host and user account (https://knowledgebase.constantcontact.com/articles/KnowledgeBase/5632-security-of-my-data-on-constant-contact-servers).

9. Access to personal information from outside of Canada is limited to authorized personnel. Perspective students have provided implied consent by entering their information.

Reasons

1. While traveling outside of the country, access is necessary for university administrators, researchers and other employees to perform their assigned duties or as a necessary part of a research project.

2. Prior to the Office 365 implementation faculty/staff & students were already using cloud based storage and email on the Acadia network (Google/DropBox). This enables Acadia to have greater security over the file shares.

3. The functionality is essential to the ongoing needs of the University with respect to event management and registration. It was determined that security and privacy provided by Attend.com meets the needs of the University, and no Canadian solution provided the required functionality.

4. The product has been determined to be the best fit for the Divinity College and is widely used in Canada.

5. Access to information is necessary for students to complete their course work and for faculty and staff to support the students. Decisions to allow students to access their course material and relevant data are maintained within Open Acadia/Divinity College and the course/instructor level. Faculty/staff and student access is based on authenticated login credentials.

6. Team Dynamix is the industry standard for ticketing and project management in the higher education sector.

7. Employees require access to input or view data while traveling. It is a core component of their activities. The information is required for the success of Advancement and its events. Employees require access to their time reporting, payroll and T4 information from both on and off campus.

8. Constant Contact is the industry standard for communication and mass email distribution within the sector.

9. eZRecruit is a viable cost effective solution that integrates with our student information system. It has a proven track record within the higher education industry

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 from a distance. 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. SchooiDude: SchooiDude is a cloud-based ticket tracking system used by CBU's Facilities Management Department. The SchooiDude 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.; Dublin, Ireland; and Sydney, Australia. Personal information of CBU contacts and prospective and current systems are held in HubSpot's cloud-based data centres outside Canada. The Marketing and Communications Department has determined that no Canadian solution exists that will provide the functionality of HubSpot, and that use of the system is necessary to the operations of the Department.

9. Destiny One: Destiny One is a system used by CBU to assist in delivery of open learning courses available to non-CBU students. Destiny One is a cloud based system operating through Amazon. Data stored in the system is currently housed in Amazon Data Centres in the US.

While no Canadian system could initially be found to provide the required functionality, Amazon will be opening its Canadian Data Centre in the next year, and all Canadian clients including CBU will be moved to this centre. Currently, data kept in the system is the minimum required for the delivery of these courses.

10. Office365: In the past year, CBU has implemented Office365 for all employees and students. While CBU data in the 0365 cloud is maintained in Microsoft's Canadian Data Centre, all users have access to their data from anywhere in the world where internet access is available.

11. Travel: CBU faculty and staff participated in approximately 50 international trips to 16 different countries in 2016. 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 Share Point sites. While travelling outside the country, such access is necessary for university administrators, researchers, and other employees to perform their assigned duties or as a necessary part of a research project.

Conditions

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

2. **Storage** of personal information outside Canada. 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

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

2. **Storage**: The user Department has determined that security and privacy provided by the product 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[12]

Description

1. **Undergraduate Medical Education Exam System**
   This system is a student assessment management solution that supports the entire testing process, including exam creation, administration, delivery, scoring, and analysis

2. **Community Health & Epidemiology (CH&E) Process Improvement**
   Sharepoint 2013, a collaboration software product within Office 365, is used within my.dal.ca to allow document sharing, file management and collaborative authoring between the CH&E Department and the Maritime SPOR Network

3. **Continuing Education Software**
   Destiny One is a software system that streamlines business processes, increases student engagement and facilitates growth for Continuing Education divisions across North America. It allows Continuing Education departments to registrar students for courses that do not follow the traditional University schedule.

4. **Lecture Capture & Streaming Media Solution**
   This software allows academic institutions to record, webcast, and search all of their video content and presentations.

5. **ACHA-NCHA National College Health Assessment Student Survey**
   This internationally recognized student survey is the mechanism for Dalhousie to collect quality data about students' health habits, behaviours, and perceptions, allowing Dalhousie to better understand and address the needs of students for services, education and programming related to their physical and mental health.

6. **Plagiarism Detection Software**
   This product is a fully automated system for handling plagiarism, which checks documents against four central source areas: the Internet, published material, Dalhousie Student material and global student material.

7. **Educational Technology Apps**
   Both the grader and binder app provide users the ability to conduct teaching and learning activities on a mobile device. The Grader App allows instructors to move documents off the Brightspace LMS and onto a mobile device for grading purposes, while the Binder app allows materials on the LMS to be viewed and annotated by students or faculty on laptops or mobile devices.

8. **Insights, Pulse, Wiggio and Video Note**
   The following tools are components of the Brightspace learning management system**:**
   - **Insights** is an advanced analytics tool that allows the University to capture learner data and produce reporting that will help predict and measure student performance**.**
   - **Pulse** is a mobile app that helps students manage their workload with real time alerts for course due dates, etc.
   - **Wiggio** is a group communication and collaboration tool.

[12] Report includes the Nova Scotia Agricultural College

- **Video note** is a tool that allows instructors to record and embed videos into Brightspace.

9. **Web-Based RCT Platform.**
   See description of storage provided in the 2015 annual PIIDPA report.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Conditions

1. **Undergraduate Medical Education Exam System**
    - A Service level agreement and a non-disclosure agreement contain privacy and confidentiality obligations.
    - User access controls are in place and periodic auditing of user access will be done by the Undergraduate Medical Education Office.

2. **Community Health & Epidemiology (CH&E) Process Improvement**
    - Dalhousie and Microsoft have executed online service agreements that provide protection for personal information (e.g. protections against loss or misuse of this information).
    - Microsoft meets a number of recognized security and privacy standards (ISO 9001, ISO 27001 and ISO 27018) and are audited annually against these standards.

3. **Continuing Education Software**
    - The service provider has extensive policies, procedures and guidelines to protect the privacy and security of information.
    - Contractual obligations limit data use to approved purposes and specify protections for confidential information.

4. **Lecture Capture & Streaming Media Solution**
    - Contractual obligations and a non-disclosure agreement protect the confidentiality of information
    - The service provider has in place internal safeguards that protect the information from accidental loss, unauthorized access or disclosure.
    - The University has in place guidelines and training for faculty to help them minimize the privacy impact to students when recording lectures (e.g. do not call students by their full name, cameras are to be focused on the faculty member only)

5. **ACHA-NCHA National College Health Assessment Student Survey**
    - Servers are protected by high-end firewall systems, and system vulnerabilities are identified through regular scans and penetration testing.
    - The identifiable data stored is limited to student's email address.
    - Data in transit is encrypted using industry standards
    - Access to data is restricted and audited for compliance.
    - Policies are in place to ensure identifiable data is not shared with other parties, used for another purpose, or retained longer than necessary.
    - A data agreement is in place to protect the confidentiality of the data
    - A unique survey link, connected to a random Response ID number, make it difficult to link survey responses to a particular email address

6. **Plagiarism Detection Software**
    - The service provider's servers are protected by firewalls and communication to and from them is encrypted.
    - User access controls are in place to limit employee access to the information they need to do their jobs and an auditing strategy is in place.
    - Contractual obligations and a non-disclosure agreement protect the confidentiality of information.

7. **Educational Technology Apps**
    - A master agreement is in place with the service provider, which includes confidentiality and privacy obligations.
    - Microsoft Azure, a US based hosting service, meets a number of recognized security and privacy standards (SOC 1, SOC 2, ISO 27001 and ISO 27018) and are audited annually against these standards.

8. **Insights, Pulse, Wiggio and Video Note**
   - These components store data outside of Canada with Amazon Web Services (AWS), which has been certified as meeting a number of security standards (e.g. SOC1, SOC2, SOC3, ISO 27001)
   - Measures include firewalls, encryption of data in transit, user access controls and an acceptable use policy.
   - Contractual obligations protect the confidentiality of information.

9. **Web-Based RCT Platform.**
   See description of storage provided in the 2015 annual PIIDPA report.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

<u>Reasons</u>

1. **Undergraduate Medical Education Exam System**
   Replacement of the traditional paper based system for undergraduate medical student examinations with a software solution was necessary to:
   - permit students to take examinations simultaneously in multiple sites across the Maritimes in an efficient manner;
   - provide comprehensive learning analytics and reporting to support ongoing enhancement to the assessment practices for learners.
   - No Canadian alternatives were identified as part of the formal procurement process.

2. **Community Health & Epidemiology (CH&E) Process Improvement**
   - There was an operational need for collaboration tools, a central location for management of requests, and shared reporting capabilities, where the groups use two separate computer networks.
   - Dalhousie previously approved the use of Microsoft Office 365 through a process that did not identify any alternative cloud based solution that stored or accessed the information in Canada.

3. **Continuing Education Software**
   - Legacy systems were no longer supportable.
   - No Canadian alternatives were available

4. **Lecture Capture & Streaming Media Solution**
   - Dalhousie did not have a streaming media server or institutional lecture capture solution to support the use of video as a teaching tool.
   - No Canadian hosted video storage solutions were identified.

5. **ACHA-NCHA National College Health Assessment Student Survey**
   - There is no Canadian alternative that provides the same breadth of information
   - The ACHA-NCHA survey is the accepted standard tool for Canadian institutions, allowing the university to compare its results to aggregate data from over 30 other Canadian universities and colleges.

6. **Plagiarism Detection Software**
   There is no alternative plagiarism detection software that stores data inside Canada.

7. **Educational Technology Apps**
   There is no other Canadian alternative, as these are the only apps of this nature available through the Brightspace system.

8. **Insights, Pulse, Wiggio and Video Note**
   - These components provide functionality that is key to Dalhousie's e-learning environment. For example, Insight's learner analytics allows the University to support students and develop retention strategies in a new and transformative way.
   - No Canadian product offered a comparable suite of products, service and functionality.

9. **Web-Based RCT Platform.**
   See description of storage provided in the 2015 annual PIIDPA report.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Mount Saint Vincent University

Description

1. **NSSE Survey**

During 2016, Mount Saint Vincent University participated in the National Survey of Student Engagement (NSSE) project facilitated by the Indiana University, through the Indiana Center for Postsecondary Research, and in cooperation with the Indiana University Center for Survey Research by supplying Indiana University with a data file containing certain personal information of undergraduate students in their first year of study and undergraduate students in their final year of study at the University; Indiana University then invited students to participate in the NSSE. A research agreement was developed and used to facilitate the Mount's participation in the NSSE Survey.

The Mount provided the identifiable personal information to Indiana University, subject to the terms and conditions of the Research Agreement and to the provisions of the *Nova Scotia Freedom of Information and Protection of Privacy Act* (FOIPOP) and the *Personal Information International Disclosure Protection Act.* It was agreed that:

- For the purposes of protecting confidentiality of the student information, and the protection of students' personal privacy that the collection, use and disclosure of students' personal information be restricted as per FOIPOP Section 29.

- As per FOIPOP Subsection 29(a), the research purpose cannot reasonably be accomplished unless Indiana University has access to individually identifiable personal information.

- As per FOIPOP Subsection 29(b), the personal information will not be linked to any other database.

- As per Section 29(c), the President of Mount Saint Vincent University has approved conditions agreed to by Indiana University with respect to: 1) security and confidentiality; 2) the removal or destruction of individual identifiers at the earliest reasonable time; and 3) the prohibition of any subsequent use or disclosure of that information in individually Identifiable form without the express authorization of MSVU.

2. General

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.

Conditions

1. NSSE Survey

The research agreement with the Indiana University for the Mount's participation in the NSSE Survey stipulates:

- Indiana University shall not disclose any personal information about any individual obtained in the course of administering the NSSE to any other person or organization. All personal information gathered or obtained by Indiana University will be treated as confidential and kept in a physically secure location to which only the necessary NSSE research staff have access, and no personal information will be used or disclosed in a manner in which the students to whom it relates could be identified. Any research report resulting from the survey will contain information in a statistical summary or anonymous format that precludes the identification of any individual.

- Indiana University shall immediately advise in writing the Vice-President - Academic of the Mount in the event that it receives a formal or legal demand or request for access to, or disclosure of, any personal information submitted by the Mount.

- Indiana University will notify the Mount immediately upon becoming aware that any term or condition of this agreement has been breached or if a privacy breach results in inadvertent disclosure of students' personal information.

- Indiana University will not link or combine personal information with personal information or data obtained from any other source.

- The Mount reserves the right to audit compliance with this agreement.

- Indiana University will destroy all paper and electronic records of the email addresses once the 2017 NSSE is completed. Indiana University will destroy all paper and electronic data that links the information to a particular individual within six months of completion of the 2017 NSSE.

2. General

The information they (e.g., a student, faculty or staff member) have access to is maintained on a server controlled by Mount Saint Vincent University (within Canada).

Reasons

1. **NSSE Survey**

The results of the research will help the Mount identify aspects of the student experience that should be improved in order to improve or enhance the Mount's programs of study and student support services. The parties believe that it is in the public interest for universities to have information that will assist them in improving the student experience both inside and outside the classroom.

2. **General**

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 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

1. Our primary vehicle for email, collaboration and personal storage is Microsoft Office 365. The decision to use this product was made several years ago and it has now become the standard for Universities in the Province of Nova Scotia. As a group, the Universities in Nova Scotia continue to negotiate with Microsoft to have all functional storage moved to data centers in Canada, an initiative that Microsoft has agreed to in principle.

2. The University supplies mobile equipment such as laptops, tablets and smart phones to specific University personnel who travel on behalf of the organization or who otherwise may be required to connect in cases of emergency.

3. The University provides access to certain information via various web interfaces and virtual private networks (VPN) from anywhere in the world as required to carry on its business.

Conditions

1. Office 365 provides the ability for individual employees and students to make the decision on what information they store. The University provides training on security and privacy and further provides alternative file services and methodologies that remain on campus.

2. Laptops provided by the University are encrypted and secured by Computer Services. All users are encouraged to use provided storage mechanisms that do not place information directly on the device.

3. Access to information is limited in most cases to one's own personal information protected by robust authentication. Access directly to our information databases is restricted to those who must have it to perform their jobs and is provided through access to a virtual private network. NSCAD University continuously reviews and refines access to information by all system users to determine how that information can best be secured and what information is necessary for job performance.

Reasons

1. Office 365 has become a standard tool for Universities in Nova Scotia. Functionally, it has improved the ability of users to communicate and collaborate, and has an enhanced feature set when compared to other products. In addition the combination of a large dedicated vendor and a collaborative approach to management by N.S. Universities provides better security than could otherwise be expected.

2. Mobile devices are replacing traditional means for accessing data and job performance. The trends transcend the abilities of Universities to restrict their use or access to information through policy or technology. Universities in Nova Scotia have decided to combine the best use of available technology for data protection with user education on security and privacy.

3. NSCAD University like most, recruits and collaborates internationally. International students and employees who travel on behalf of the organization must have access to information for

the university to function. NSCAD University provides tested and proven means of access that are technically sound and designed to provide information necessary to the function being performed. In this regard NSCAD University works continuously with partner institutions and vendors.

Nova Scotia Community College

Description

As required by section 5(3) of the *Personal Information International Disclosure Protection Act (PIIDPA)* the Nova Scotia Community College (NSCC) is reporting that it has allowed for the storage of personal information under our control to be stored on servers located outside of Canada.

1. In 2016, NSCC completed its migration of electronic mail to Microsoft Office 365 in collaboration with the Higher Education Information Technology Shared Services (HISS) organization. HISS is funded by the Province of Nova Scotia to facilitate initiatives of this nature for all post-secondary education institutions in the province. During the year, Microsoft opened two data centre facilities in Canada and in October 2016, NSCC formally requested that Microsoft migrate NSCC data to their Canadian data centres in the next 24 months.

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

3. For accessing personal information in NSCC 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 cannot prevent it. The College is planning to promote Microsoft's OneDrive for Business offering as an alternative as this will keep data in Canada following the aforementioned migration.

Conditions

See above description.

Reasons

See above description.

St. Francis Xavier

Description

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

2. Kinetics Software: 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. Everbridge: See description of access and /or storage provided in the 2015 annual PIIDPA report.

7. WC Online: See description of access and /or storage provided in the 2015 annual PIIDPA report.

8. St. FX uses a survey tool provided by Qualtrics which is a US owned company head quartered in Provo Utah. Data of Canadian clients is stored in Ireland. Surveys are used for research and teaching purposes.

9. FluidReview is used to for the management of the Universities scholarship program. FluidReview, which is owned by US based SurveyMonkey, is located in Ottawa, ON. All data is stored in Canada.

10. Employees Travelling email. Employees who travel will be required to take all reasonable precaution to protect personal information.

Conditions

1. Remote Access to the OneSolution Server is controlled by StFX through the gateway program. Access is limited to maintenance and program updates and all activity is logged and reviewed by external auditors.

2. See conditions for access and/or storage provided in the 2014 annual PIIDPA report.

3. See conditions for access and/or storage provided in the 2014 annual PIIDPA report.

4. See conditions for access and/or storage provided in the 2014 annual PIIDPA report.

5. See conditions for access and/or storage provided in the 2014 annual PIIDPA report.

6. See conditions for access and/or storage provided in the 2015 annual PIIDPA report.

7. See conditions for access and/or storage provided in the 2015 annual PIIDPA report.

8. Access to Qualtrics 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. Qualtrics users inform participants of privacy issues and obtain consent for the use of information supplied.

9. Access to FluidReview 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.

10. Email data accessed by travelling employees is protected and limited to authorized users through industry standard data security, encryption, and authentication practices.

Reasons

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

2. See reasons for access and/or storage provided in the 2014 annual PIIDPA report.

3. See reasons for access and/or storage provided in the 2014 annual PIIDPA report.

4. See reasons for access and/or storage provided in the 2014 annual PIIDPA report.

5. See reasons for access and/or storage provided in the 2014 annual PIIDPA report.

6. See reasons for access and/or storage provided in the 2015 annual PIIDPA report.

7. See reasons for access and/or storage provided in the 2015 annual PIIDPA report.

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

9. The Vendor was chosen for best meeting operational needs, functionality, data security and cost as compared to known alternatives.

10. Access to email while traveling outside of the country is required by employees to meet the operational requirement of their positions.

St. Mary's University

Description

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

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

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

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

5. Saint Marv's University Commercial Card Program: See description of access or storage provided in the 2014 annual PIIDPA report.

6. Evernote: See description of access or storage provided in the 2015 annual PIIDPA report.

7. DropBox: See description of access or storage provided in the 2015 annual PIIDPA report.

8. Go To Meeting/Go To Webinar: See description of access or storage provided in the 2015 annual PIIDPA report.

9. Mailchimp: Used for communication and promotion. Stores names and emails for newsletters to students, faculty, staff, leads, and business community. Helps track levels of interest and success of marketing and communications. Also used to collect leads from the website- names, emails, programs of interest. Used to ensure CASL compliance and for reliability and ease of use.

10. StarRez: Is a system used to manage campus residences.

Conditions

1. See restrictions or conditions provided in the 2012 annual PIIDPA report.

2. See restrictions or condition provided in the 2012 annual PIIDPA report.

3. See restrictions or conditions provided in the 2014 annual PIIDPA report.

4. See restrictions or conditions provided in the 2014 annual PIIDP A report.

5. See restrictions or conditions provided in the 2014 annual PIIDP A report.

6. See restrictions or conditions provided in the 2015 annual PIIDP A report.

7. See restrictions or conditions provided in the 2015 annual PIIDP A report.

8. See restrictions or conditions provided in the 2015 annual PIIDP A report.

9. The only information uploaded is first name, last name and email address.

10. Data is stored and secured on University servers but for purposes of upgrades or database problems there is occasional access by the US-based StarRez. Access is supervised by University ITSS staff.

Reasons

1. See details provided in the 2012 annual PIIDPA report.

2. See details provided in the 2012 annual PIIDPA report.

3. See details provided in the 2014 annual PIIDPA report.

4. See details provided in the 2014 annual PIIDPA report.

5. See details provided in the 2014 annual PIIDPA report.

6. See details provided in the 2015 annual PIIDPA report.

7. See details provided in the 2015 annual PIIDPA report.

8. See details provided in the 2015 annual PIIDPA report.

9. The product meets the following business communication needs:
    - CASL compliance - by allowing an unsubscribe / manage function, as well as clearly indicating reason for contact.
    - Reliable, professional, fast service. Using the on-shore product, we were able to locate in the past, as we encountered glitches, with timely delivery and bugs which caused information to reach our students too late, for instance. In another example, we encountered design and template snags that caused our communications to appear unprofessional.
    - Communications must be mobile. Again, the past product advertised "mobile-ready" but was unable to deliver a clear, professional mobile experience.
    - A consistent platform to begin to share business contacts and program leads. While a CRM project will eventually serve this need, currently, Banner does not contain business relationship information, nor grad program leads. Mailchimp enables us to begin the process of exploring how to share information with our colleagues in the Alumni and Development offices, or with our programs such as the PhD, EMBA or the MScCDA.

10. This system meets the operational requirements of the University, in an efficient and cost effective manner.

Université Sainte-Anne

Description

1. Blackbaud: Student information system that has information stored on servers 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 and access courses and course materials. Access is protected via password, but access can be from anywhere in the world.

3. Email: Our e-mail system is via Office 365 and therefore stored in the cloud. Employees and students can access the e-mail system via smartphone, tablet of computer from anywhere in the world.

Conditions

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

2. Moodle: Professors and students access course information that is stored in Nova Scotia on our servers via computer. Access is password protected.

3. Email: Access is password protected.

Reasons

1. Blackbaud: Required to assure daily operations of the Université.

2. Moodle: Required to assure daily operations of the Université.

3. E-mail: Required to assure daily operations of the Université.

University of King's College

Description

Only additions to our 2015 PIIDPA report:

1. **Educational Technology Apps**
   Both the grader and binder app provide users the ability to conduct teaching and learning activities on a mobile device. The Grader App allows instructors to move documents off the Brightspace LMS and onto a mobile device for grading purposes, while the Binder app allows materials on the LMS to be viewed and annotated by students or faculty on laptops or mobile devices.

2. **Insights, Pulse, Wiggio and Video Note**
   The following tools are components of the Brightspace learning management system:

- **Insights** is an advanced analytics tool that allows the University to capture earner data and produce reporting that will help predict and measure student performance.
- **Pulse** is a mobile app that helps students manage their workload with real time alerts for course due dates, etc.
- **Wiggio** is a group communication and collaboration tool.
- **Video note** is a tool that allows instructors to record and embed videos into Brightspace.

3. For all others: See description of access and/or storage provided in the 2015 annual PIIDPA report

Conditions

1. A master agreement is in place with the service provider, which includes confidentiality and privacy obligations. Microsoft Azure, a US based hosting service, meets a number of recognized security and privacy standards (SOC 1, SOC 2, ISO 27001 and ISO 27018) and are audited annually against these standards.

2. These components store data outside of Canada with Amazon Web Services (AWS), which has been certified as meeting a number of security standards (e.g. SOC1 , SOC2, SOC3, ISO 27001). Measures include firewalls, encryption of data in transit, user access controls and an acceptable use policy. Contractual obligations protect the confidentiality of information.

3. For all others: See description of access and/or storage provided in the 2015 annual PIIDPA report

Reasons

1. There is no other Canadian alternative, as these are the only apps of this nature available through the Brightspace system.

2. These components provide functionality that is key to King's e-learning environment. For example, Insight's learner analytics allows the University to support students and develop retention strategies in a new and transformative way. No Canadian product offered a comparable suite of products, service and functionality.

3. For all others: See description of access and/or storage provided in the 2015 annual PIIDPA report.

Foreign Access and Storage by School Boards[13]

Annapolis Valley Regional School Board

Description

1. Travel outside of Canada with electronic devices: Six AVRSB staff members received permission to use work-issued electronic devices such as cell phones, tablets and laptop computers for business continuity purposes during travel outside of Canada.

2. Advanced Placement Program: See description of access and/or storage provided in the 2015 annual PIIDPA report.

3. Use of social media: AVRSB and school Twitter accounts are used to share news, information videos and photos. Twitter is based in the United States.

4. Khan Academy: See description of access and/or storage provided in the 2015 annual PIIDPA report.

5. Google Apps for Education: See description of access and/or storage provided in the 2015 annual PIIDPA report.

6. Aesop System: See description of access and/or storage provided in the 2015 annual PIIDPA report.

7. International Baccalaureate Diploma Program: See description of access and/or storage provided in the 2015 annual PIIDPA report.

Conditions

1. See conditions of access and/or storage provided in the 2015 annual PIIDPA report.

Reasons

1. See reasons for access and/or storage provided in the 2015 annual PIIDPA report.

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

Cape Breton-Victoria Regional School Board

Description

1. The School Board along with several schools operates two social media accounts: Twitter and Facebook. Twitter/Facebook are based in the United States. These accounts are used for sharing School Board news releases, videos, photo sand 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.

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 down loaded 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.

5. Travel with electronic devices: a number of CBVRSB staff travelled outside of Canada for business and pleasure with electronic devices including cell phones, ipads and laptops. In order to take such devices across the border, the staff member needs consent from the head of the public body.

6. Google Apps for Education: CBVRSB students, teachers, and administrators use Google Apps for Education. Users can use Google Apps to create documents, slideshows, spreadsheets, etc. They can also use Google Apps for Education for storing these documents, for emailing people, to store their contacts, to manage their calendars, etc.

Conditions

1. The School Board administration and schools use social media (Twitter/Facebook) 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. 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.).

5. Remote access to cell phone and email accounts is handled through Google's email client. Staff members are required to have written permission to obtain a cell phone or data package on their cell phones prior to crossing the Canadian border.

6. All users of Google Apps for Education (GAFE) are required to have a password that is complex to help mitigate the risk of loss of personal information. Also, all student accounts are created to be non-identifying of age or gender.

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 or Facebook.

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 internationally accepted qualifications for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

5. Staff members are still required to monitor their email while they are out of the country. Depending on the nature of the trip, the staff member may also need to access the internet to visit websites to participate in conferences, workshops, training, etc.

6. Google Apps for Education is a suite of apps that is used as a productivity tool by students, teachers, and administrators. The tools allow for unprecedented collaboration for all of its users in Nova Scotia. It is used by all school boards and has a provincial committee that reviews its use. The tools that Google Apps provide are not connected to the type of device which makes it not only easy to use but more accessible as well.

Chignecto-Central Regional School Board

Description

1. Travel with Electronic Devices: See description of access and/or storage provided in the 2015 PIIDPA Report.

2. Coding with Chrome - Chrome Extension: Learn, improve or teach coding skills through Javascript, blockly, arduino, Lego EV3, etc. May be used with Lego Robotics, Sphero Robots, Etc. To study and utilize different coding languages (depending on the resource they are attempting to control).

3. Tynker App for Chrome and website: Cool characters introduce code blocks and how to use them. Short clips demonstrate common actions such as deleting actors or changing the background. You can preview game you build in each lesson and play bonus games along the way.

4. DocHub - extension and website. Edit, send and sign PDFs online for free. Students and teachers may utilize this site/chrome extension for productivity purposes.

5. Use of Social Media: See description of access and/or storage provided in the 2015 PIIDPA Report.

6. AESOP: See description of access and/or storage provided in the 2015 PIIDPA Report

7. Showbie is an App available for IOS, Android, Chrome and Windows that allows teachers with 1-to-1 classroom environments to set up a paperless learning management system that is Universal Design for Learning friendly. It is an exceptionally seamless option for classroom teachers/resource teachers to deliver accessible digital content to students with disability using accessible digital devices to access and engage in the curriculum.

8. The Brainology program teaches the growth mindset - the view of intelligence as malleable. Students come to see effort as a positive quality needed for anyone to achieve his or her full potential. They come to understand how to approach studying and learning in ways that make their brains smarter. They learn how to approach success and learn from failure.

9. CloudLab develops a number of tools for workflow and assessment in the Google Apps for Education platform. The tools are specifically third-party add ons and extensions for Google Docs, Sheets, Forms and the Chrome Browser.

10. Google Photo stores, manages and edits photos. Working with and using images allows students to enhance work and help avoid copyright. It also connects with their surroundings in the learning environment. This is a free service.

11. Google Cast for Education is a Chrome extension that allows student in GAFE to broadcast their screens to a teacher's computer. Useful in a classroom with mobile devices, such as Chromebooks, when teachers want to project student work in a controlled manner.

12. Explain Everything App for Chrome. It is an online interactive whiteboard for the production of videos using video footage, sounds, characters, drawings, etc.

13. MIT Appinventor is a beginner's introduction to programming and app creation that transforms text-based coding into visual, drag and drop building blocks and can be used by teachers and students.

14. SPRK Lightning Lab-Chrome App is the Sphero App for programming Sphero robots.

15. Kidblog: See description of access and/or storage provided in the 2015 PIIDPA report.

16. Plickers. See description of access and/or storage provided in the 2015 PIIDPA report

17. World Math Day. See description of access and/or storage provided in the 2015 PIIDPA Report.

18. Future Goals - Hockey Scholar by Everfi. See description of access and/or storage provided in the 2015 PIIDPA report.

19. Pixlr Editor is browser photo editor to be used by students or teachers.

Conditions

1. See conditions of access and/or storage provided in the 2015 PIIDPA Report.

2. None.

3. Students and teachers for learning and basic coding skills by teachers for students in P-8. May use Google authentication which means the app has access to students email address.

4. The chrome based tools will ask for permission to access the users gnspes email as a basic profile information. However, the Terms of Use specify that the access is required for the tools to operate and do not collect or store personal information other than your email if you request to receive emails from the specific tools.

5. See conditions of access and/or storage provided in the 2015 PIIDPA Report.

6. See Conditions of access and/or storage provided in the 2015 PIIDPA Report.

7. Teachers and GAFE administration use the tools for management and classroom workflow. Students may use Goobric Web Page launcher for viewing interactive rubrics. No additional identifying personal information is required to use the tool.

8. The resource can be used by a student in grades 4-9 under the direction and supervision of a teacher. Children are only allowed to register if they have a valid access code provided by someone who has obtained one from Mindset Works. If the child has a valid access code but there is no parent or legal guardian consent, they only collect personally non-identifiable information about the child.

9. There is a Privacy Policy and a Terms of Use Agreement. The only stipulation incumbent on staff is that for students who are minor, the school/board is responsible to inform parents that particular teachers will be using the service in conjunction with their student. No additional personal information is required.

10. Email process for login requires a student email and a password only. Uncertain software seems to be directly connected to Google.

11. The tool only requires a GAFE email to identify users and is only available to Google Apps for Education users under Google Terms of Use.

12. There are annual prices. The app is authenticated through GNSPES; email address collected at the registration stated. If you are a student, your user profile may only include your name. This user profile information will be displayed to other users to facilitate user interaction within the service or facilitate interaction with the company.

13. None.

14. The robots that the app connects to have costs associated with them. There is an option to create an account but this is for access to lessons and activities.

15. See conditions of access and/or storage provided in the 2015 PIIDPA report.

16. See conditions of access and/or storage provided in the 2015 PIIDPA report

17. See conditions of access and/or storage provided in the 2015 PIIDPA report.

18. See conditions of access and/or storage provided in the 2015 PIIDPA report.

19. None.

<u>Reasons</u>

1. See reasons for access and/or storage provided in the 2015 PIIDPA Report.

2. Code with Chrome would be a complementary tool to enhance the learning experience that is currently taking place in the classroom utilizing iPad apps. This tool is free and no personal information is required.

3. A very engaging platform for learning to code. Easy to use with helpful tutorials. The tool is free for basic use. No additional identifying personal information is required to use the tool.

4. Supports use of teacher created PDF files such that students are unable to make changes to the text of the file. Free limited service. May be used for assessment purposes.

5. See reasons for access and/or storage provided in the 2015 PIIDPA Report.

6. See reasons for access and/or storage provided in the 2015 PIIDPA Report.

7. Showbie is accessible by all learners and is available at no cost for students. There is no other options which is as user-friendly for all involved and is accessible for all students (from a Universal Design for Learning Approach).

8. The tool can be used without students real names, and parental consent is required for any personal information to be collected. There is no similar service available that is based on a server in Canada.

9. CloudLab's website and GAFE applications comply with the US Family Educational Records and Privacy Act (FERPA).

10. There were no alternatives identified with data storage in Canada.

11. It supports the integration of technology and the use of digital tools to maximize classroom time and provide meaningful feedback to students.

12. Explain Everything would be a complementary tool to enhance learning experience that is currently taking place in the classroom.

13. No acceptable alternative within Canada. It is a free App.

14. No identifying personal information is required to use the tool. There is not an acceptable alternative within Canada.

15. See reasons for access and/or storage provided in the 2015 PIIDPA Report.

16. See reasons for access and/or storage provided in the 2015 PIIDPA Report.

17. See reasons for access and/or storage provided in the 2015 PIIDPA Report.

18. See reasons for access and/or storage provided in the 2015 PIIDPA Report.

19. It has free access.

Conseil Scolaire Acadien Provincial

Description

1. Google Apps for Education-see attached DRA (Digital Risk Assessment)[14]

   Drive (including Documents, Presentations, Spreadsheets, Forms and Drawings) Sites, Gmail, Calendar, Groups and Contacts

Conditions

1. Basic information is provided for each user in order to establish an account. This information is limited to first and last name, email address and encrypted password. See attached DRA (Digital Risk Assessment)

[14] See Appendix 1.

Reasons

1. No alternatives were identified with data storage in Canada.

   Google Apps for Education support and encourage collaboration among teachers and students. The simplified, intuitive end user experience allows the focus to remain on the learning objectives, not the technology. 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.

Halifax Regional School Board

Description

See description of access and/or storage provided in the 2015 annual PIIDPA report.

Conditions

See description of access and/or storage provided in the 2015 annual PIIDPA report.

Reasons

See description of access and/or storage provided in the 2015 annual PIIDPA report.

South Shore Regional School Board

Description

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

2. **Use of Social Media**
   (a) Twitter- The South Shore operates a Twitter account. Twitter is based in the United States. This account is used for sharing government news releases, videos, photos and other information to a broader audience.

   (b) Facebook- The 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.

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 from 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 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.

5. **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.

6. **International Baccalaureate Diploma Program**
The South Shore 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 and aides in administering the program.

7. **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 attended, grade, and academic achievement is disclosed by the School Board to the College Board to administer the program.

Conditions

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

2. **Use of Social Media**
(a) The South Shore Regional School Board uses Twitter to share information and interact online with the 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 to all social media platforms have written consent from the people in them where required.

3. **Khan Academy**
   It is recommended that teachers set up Khan Academy student accounts so that students, under the age of 13 can post comments, change their password, etc.

   It is recommended that a minimum amount personal information is provided about students and teachers at the point of setting up new accounts. For example, it was recommended that the birth and teachers were fictitious, and the field indicating gender was left blank. It was recommended that usernames be the student's or teacher's three initials plus 5-6 numbers, to reduce the ability to easily identify an individual, their gender, or ethnicity.

4. **Google Apps for Education**
   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. **Aesop**
   The Department of Education and Early Childhood Development and the South 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 Protection Act. The contract also has extensive provisions 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.

6. **International Baccalaureate Diploma Program**
   Parents/guardians receive information about the IB program, including that it is administered outside Canada (Switzerland, UK, etc.).

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

Reasons

1. **Travel with electronic devices**
   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 needed for preparing documents, and accessing email and Internet sites.

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

3. **Khan Academy**
   It is essential that the education system engages and motivates students, protects rural education, provides information and resources teachers need, links learning to the workplace, and strengthens skills that help students. The Khan Academy is an opportunity to infuse classrooms with technology-based learning that will enhance the overall education experience, particularly in the area of mathematics.

   There is no acceptable equivalent located within Canada to the Khan Academy. Such access and storage is authorized through determination of "necessity" under S. 5(2) of PIIDPA.

4. **Google Apps for Education**
   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. **Aesop**
   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."

6. **International Baccalaureate Diploma Program**
   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. **Advanced Placement**
   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** – 31 staff
2. **Use of Social Media** – same as 2015 PIIDPA Report
3. **Google Apps for Education** – same as 2015 PIIDPA Report
4. **Aesop –** same as 2015 PIIDPA Report
5. **International Baccalaureate Diploma Program –** same as 2015 PIIDPA Report
6. **Advanced Placement –** same as 2015 PIIDPA Report

Conditions

1. **Travel with electronic devices** – same as 2015 PIIDPA Report
2. **Use of Social Media** – same as 2015 PIIDPA Report.
3. **Google Apps for Education –** same as 2015 PIIDPA Report
4. **Aesop** – same as 2015 PIIDPA Report
5. **International Baccalaureate Diploma Program** – same as 2015 PIIDPA Report
6. **Advanced Placement** – same as 2015 PIIDPA Report.

Reasons

1. **Travel with electronic devices** – same as 2015 PIIDPA Report
2. **Use of Social Media** – same as 2015 PIIDPA Report
3. **Google Apps for Education** – same as 2015 PIIDPA Report
4. **Aesop** – same as 2015 PIIDPA Report
5. **International Baccalaureate Diploma Program** – same as 2015 PIIDPA Report
6. **Advanced Placement** – same as 2015 PIIDPA Report

Tri-County District School Board

Description

1. **Travel with electronic devices**
   A number of Tri-County 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 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 Tri-County operates a Twitter account. Twitter is based in the United States. This account is used for sharing government news releases, videos, photos and other information to a broader audience.

   b. Facebook – The Tri-County uses also uses Facebook as a professional communication tool to engage the school community and share relevant information to parents, teachers, students and the public. Facebook is based in the United States.

3. **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. **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.

5. **International Baccalaureate Diploma Program**
   The Tri-County 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 to administer the program.

6. **Media Release**
   Parents or guardians of Tri-County Regional School Board students sign media releases, enabling the student's picture, school work, or other articles of information, to be shown on our TCRSB website, shared with the School Board Members, or featured in a local newspaper or news website.

Conditions

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

2. **Use of Social Media**
   a) The Tri-County uses Twitter to share information and interact online with the public and organizations in social spaces. The Tri-County collects no IP addresses or personal information through these services. The Tri-County 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.
   c) Photos and videos that are posted to all social media platforms have written consent from the people in them where required.

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

   It is recommended that the minimum personal information is provided about students and teachers at the point of setting up new accounts. For example, it is recommended that the birth dates entered for all students and teachers were fictitious, and the field indicating gender was left blank. It is recommended that usernames be the student's or teacher's three initials plus 5-6 numbers, to reduce the ability to easily identify an individual, their gender, or ethnicity.

4. **Aesop**
   The Department of Education and Early Childhood Development and the Tri-County Regional School Board has four years remaining in a 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 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.

5. **International Baccalaureate Diploma Program**
   Parents/guardians receive information about the IB program, including that it is administered outside Canada (Switzerland, UK, etc.).

6. **Media Release**
   None. If information were stored on a website, it could be accessed anywhere in the world.

<u>Reasons</u>

1. **Travel with electronic devices**
   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, and make telephone calls. Laptops and other devices are needed for preparing documents, and accessing email and Internet sites.

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

3. **Khan Academy**
   It is essential that the education system engages and motivates students, protects rural education, provides information and resources teachers need, links learning to the workplace, and strengthens skills that help students. The Khan Academy is an opportunity to infuse classrooms with technology-based learning that will enhance the overall education experience, particularly in the area of mathematics.

   There is no acceptable equivalent located within Canada to the Khan Academy. Such access and storage is authorized through determination of "necessity" under S. 5(2) of PIIDPA.

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

5. **International Baccalaureate Diploma Program**
   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. **Media Release**

The Tri-County Regional School Board (TCRSB) believes that celebrating students and their achievements is an important part of school life and can be a very positive experience, leading to the sharing of ideas, collaboration on projects, and a sense of pride. We also believe in the need to protect all students and recognize the issues surrounding the publishing of student information. At various times throughout the year, the board or individual schools may create media highlighting school events, classroom work, and student achievements. These may contain a student's name, classroom, and their school name in publications.

Foreign Access and Storage by Municipalities[15]

Cape Breton Regional Municipality [16]

Description

1. We do not store any CBRM data outside the country. We currently do not allow our data to be stored outside the country. However, staff do travel outside the country on occasion and do access CBRM information from their electronic devices.

Conditions

1. We require each employee that is taking a CBRM device (laptop, smart phone, tablet) outside the country to register the dates they are traveling along with the county to the Department of Technology. All data storage is within Canada therefore no restrictions are required on storage of data.

Reasons

1. It is the practice of the CBRM to not store data outside the country, therefore this component is not an issue. Employees do take CBRM devices outside the country for work purposes and are required to register with the Department of Technology.

[15] Municipality of the County of Colchester, Municipality of the County of Cumberland, 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 Digby, Municipality of the District of St. Mary's, Municipality of the District of Shelburne, Town of Clark's Harbour, Town of Digby, Town of Lockeport, Town of Lunenburg, Town of Mulgrave, Town of Pictou, Town of Shelburne, Town of Stellarton, Town of Stewiacke, Town of Trenton, Town of Westville, Town of Windsor, the Cumberland Joint Services Management Authority, the Digby Area Recreation Commission, South Shore Regional Library Board, Municipality of the District of Clare, Municipality of the County of Kings, Region of Queens Municipality, Town of Antigonish, Town of Berwick, Town of Oxford, and Town of Port Hawkesbury did not have access or storage outside of Canada to report.

[16] Report includes Cape Breton Regional Police Service.

Halifax Regional Municipality[17]

Description

1. Between January 1st and December 31st, 2016, twenty-three (23) HRM staff and one (1) HRP staff travelled outside of Canada to the United States, five (5) HRM staff and one (1) HRP staff travelled outside of Canada to Europe and one (1) HRM staff travelled outside of Canada to the Caribbean 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 & City Works) 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. 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.

[17] Report includes Halifax Regional Police and the Halifax Public Library.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. Legal Case Files (Legal Case File and Matter Management System), with a headquarters in Springfield, Illinois were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

20. Intellibook Arrest Processing System were provided access on an approved need basis to the applicable production systems for support and maintenance purposes.

21. IamResponding (Volunteer Notification Solution) with a headquarters in NY.

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

23. Doodle (Scheduling Tool) a Swiss company with offices in Zurich, Berlin and Tel Aviv one time use for the scheduling of training for 1400+ temporary employees for the 2016 Municipal Election.

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

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

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

27. Explore Analytics, with a headquarters in San Jose, Ca.

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

29. Desire2Learn - Brightspace, Learning Management System, with a headquarters in Kitchener, ON.

30. Active Network Hosted Payment Server, with a headquarters in Las Vegas, NV.

31. G4S (provision of parking enforcement services) with a Canadian headquarters in Toronto, ON.

32. Typeform (Collection and sharing of information) with a headquarters in Barcelona, Spain and a data centre in the US one time use for Planning & Development, Centre Plan Project; IP addresses collected.

Conditions

1. Prior to travelling, staff were advised that HRM Communication tools (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. Service providers are bound by duly executed agreements that detail their obligations for the protection, use and disclosure of personal information, use is voluntary and instructions provided to the respondents not to include any personally identifiable information in their feedback

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

Halifax Regional Water Commission

Description

1. Between January 1 and December 31, 2016, forty-nine (49) Halifax Water staff were permitted to transport personal information devices, such as laptop computers, cell phones, and electronic data storage devices outside Canada eighty-six (86) times.

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

Conditions

1. Prior to travelling, staff were advised that Halifax Water communication tools (cell phones, 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 (no direct link to support customer account information located in SAP). Customer technical services are provided for in the annual agreement.

Reasons

1. Halifax Water owns and operates critical infrastructure as defined by Public Safety Canada. Halifax Water staff, were approved for travelling outside Canada with their communication device(s) to ensure they remained in contact with other utility staff to fulfill operational responsibilities.

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

Municipality of the County of Annapolis[18]

Description

1. In December 2016, the Warden travelled outside of Canada on personal business. He took a municipally-owned smartphone with him to access his municipal e-mail account.

2. Having been informed that our current payroll interface system would no longer be supported commencing in 2015, a decision was made to upgrade payroll services provided by ADP Canada. As a result of the upgrade, the County's payroll, overtime, vacation and sick time is stored in a new ADP product, Workforce Now. Although the data access and processing is within Canada, the server containing the information and through which the data is accessed is actually located in New Jersey, USA.

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

Conditions

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

2. All payroll and HR data access is authenticated through a secure login with password protection. The service provider (ADP) has agreed to specific safeguards which details their obligations for the protection, use and disclosure of personal information held on behalf of the County which includes requiring them to report any breaches of security or unusual access (including the *Patriot Act).*

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.

2. ADP was the better solution with the ability to grow and expand with our needs. From the perspective of business continuity planning, provision of an internet-based rather than a desktop based interface was identified as a positive step.

Municipality of the County of Antigonish

Description

1. **PathFive Recreation Software**
   PathFive Recreation Software (Dreamstalk Studios Inc., Kelowna BC); utilizes Stripe Connect as a payment tool, and clause 3.1.3 in the Terms and Conditions states:

   > *Stripe Connect may transfer, process, or store User Data outside of Canada and User Data may be subject to disclosure by Stripe Connect as required by law, as set forth in Stripe Connect's Privacy Policy.*

2. **Purely HR/Time-off Manager**
   Purely HR/Time-off Manager (IronFlow Tech Inc., Dieppe NB); servers are hosted and managed by Contegix, which identifies server locations being in US and Europe.

Conditions

1. **PathFive Recreation Software**
   No conditions are placed on the utilization of this software.

2. **Purely HR/Time-off Manager**
   Minimal personal identifying details utilized for function of program (name, email, position, start date, time-off type and dates).

Reasons

1. **PathFive Recreation Software**
   Utilizing this Canadian-based software program requires use of the Stripe Connect tool as part of the function of the program.

2. **Purely HR/Time-off Manager**
   No option to not use servers to use program - program allows greater efficiency at scale and expense acceptable to unit.

Municipality of the County of Inverness

Description

1. The CAO travelled to the US on vacation in April and October.

Conditions

1. The CAO had his iPhone with him at all times.

Reasons

1. The iPhone was necessary to keep in touch with the office.

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 device with them. During this time employees had access to the municipality's email system from their mobile device.

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 and changed on a regular basis.

Reasons

1. Employees and elected officials may request to travel outside 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 District of Chester

Description

1. Remote access via electronic devices such as iphones, ipads, and laptops. There where 4 instances in which staff members were approved to take electronic devices while travelling outside Canada. During this time staff had access to the Municipalities 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. Access to information stored on Municipal servers was accessed via electronic devices in the United States by 2 Councillors and 2 staff members. Protection of privacy protocols are followed when accessing Municipal information.

2. ReCollect.net — was deployed for effective communication and sharing of solid waste collection services. ReCollect complies with all Nova Scotia and federal privacy legislation. Specifically, with section 5 (1) of *the Personal Information International Disclosure Protection Act,* ReCollect seeks explicit consent from an individual before any data is stored in the cloud.

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

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

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 (name, address, telephone numbers, birth dates, employee numbers, etc.

Conditions

1. 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.

2. 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.

3. 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.

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

2. The storage of information on ReCollect.net was necessary to conduct business in 2016.

3. The storage of information on Wrike.com was necessary to conduct business in 2016. The Municipality of East Hants continues to explore other means of collaborative project management tools.

4. The storage of information on dropbox.com was necessary to conduct business in 2016. The Municipality of East Hants continues to explore other means of large file sharing tools.

5. The U.S. Bank has been the service provider for the Municipality of East Hants for the past 17 years.

Municipality of the District of Guysborough

Description

1. Carrying of cell phone for work during vacation. Carrying of cell phone to trade show in Texas.

Conditions

1. Used only as necessary. Used only as needed.

Reasons

1. Data was only stored on phone for the 7 days while on vacation. CAO needs to be in contact with the Office. Director of Economic Development needs to be accessible due to projects on the works. CAO needs to be available for contact to council and the office.

Municipality of the District of Lunenburg

Description

1. No personal information is consistently stored outside Canada. On an exception basis, staff or elected officials have requested permission to travel outside the country with smartphones or laptop computers, which may contain personal information contained in e-mails and electronic files. During 2016, the following such requests were authorized:
   - Two elected officials, and
   - One employee.

2. 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. Attached is information on a vendor who was provided access on an approved, need basis to the applicable production systems for support and maintenance.
   a. **Company Name and Location:** GE Water & Process Technologies. 3239 Dundas St West, Oakville, ON.

   b. **Company Description:** Provides support services to the Cookville WWTP, using InSight Pro – Process Consulting Service – Knowledge Management Solution.

   c. **Department User and Program Use:** Engineering – provides support services to the Cookville Wastewater Treatment Plant, using InSight Pro - Process Consulting Service – Knowledge Management Solution. InSight captures and transforms plant data into information needed to maximize performance, avoid operation interruptions, optimize its process, and reduce the total cost of the operation.

d. **Protocols in Place for Security:** InSight will store and maintain the Data in a secure manner and logically separate from data belonging to other customers consistently with industry standards. Data will be sorted and maintained for an archive period of 1 year, and then will be destroyed. InSight will use commercially reasonable efforts to maintain to ensure that there are no viruses, Trojan horses, trading or other cookies, malware or any other harmful software embeded in or attached to such equipment, systems, software or network interfaces.

e. **Encryption for when data moves outside of Canada:** Data is all stored in the US as that is where their main GE data centres are. They have advised that the emails that is sent from MODL site to their data centre is not encrypted. On the web, the use the https connection TLS 1.2. The connection is encrypted using AES_128_CBC, with HMAC-SHA1 for message authentication and RSA as the key exchange mechanism. All data remains subject to the confidentiality provisions set forth in their agreement.

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

Conditions

1. Where practical, access to such information has been through remote access software, allowing the actual data to remain in Canada while being available during travel. Information Technology staff have provided access devices with no personal information contained on them to facilitate such remote access.

   One elected official took their own computer which contained municipal e-mails.

   All devices are encrypted and password protected in accordance with the Municipality's standard operating procedures.

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

3. All e-mail activity is controlled or monitored by our IT support.

Reasons

1. Maintaining contact with elected officials and staff members during travel for professional development, research, and other reasons is critical to maintaining the effective operations of a municipality with limited staff resources. In the cases where storage or access to personal information has been approved, the approval considered the impact to service delivery versus the actual risk to privacy in the decision-making process.

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

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

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.

3. 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 of stolen. Also, unsuccessful passcode attempts will wipe device (10 unsuccessful attempts).

2. Access to municipal data on mobile devices outside of email is provided by the use of a VPN data connection of an SSL SharePoint site. IT administrator can revoke VPN access should the mobile device be lost of stolen. No municipal data (outside of email) is stored on the mobile device, on accesses through the 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.

3. N/A

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.
2. N/A

3. N/A

Municipality of the District of Yarmouth

Description

1. Seven 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[19]

Description

1. Two Town of Amherst staff members travelled to the United States on personal time (vacation) and had access to personal information (previous emails, email addresses) via their devices (iPhone, iPad or laptop computer). 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 EX Labour, a product offered by ADP.

Conditions

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

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.

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 of Canada.

2. Client contract agreement with ADP to ensure protection of our information.

[19] Report includes Amherst Police Department.

Town of Annapolis Royal[20]

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.

Conditions

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

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 in 2017 and consideration will be given to moving the web host to Canada.

Town of Bridgewater

Description

1. For the above noted calendar year, 1 employee travelled outside of Canada and had accessed the Town of Bridgewater information via his smartphone. This employee requested preauthorization to access his emails while away due to staffing issues and workload.

2. For the above noted calendar year, 1 employee travelled outside of Canada and had accessed the Town of Bridgewater information via his laptop. This employee requested pre-authorization to access his emails while away due to workload.

3. For the above noted calendar year, 1 Councillor for the Town of Bridgewater travelled outside of Canada 12 times (all for the same reason-job related) and had accessed the Town of Bridgewater information via his phone, tablet and laptop. This Councillor, as part of his employment, must travel outside of Canada regularly and received pre-authorization to access his emails and other information while away so that he could carry out the duties expected of him as an elected official.

[20] Report includes Annapolis Royal Police Department, Committees/Boards: Committee of the Whole, Council, Planning and Heritage Advisory Committee, Marketing and Economic Development Committee, Traffic Flow Advisory Committee, Waterfront Development Committee, Municipal Effectiveness Advisory Committee, Board of Police Commissioners, Annapolis Pool Committee, Police Services Review Committee.

Conditions

1. 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 Kentville

Description

1. Two (2) Town of Kentville councillors travelled to the United States in 2016 and accessed email on iPhone(s), iPad(s) and Laptop. CAO Approved travel. CAO travelled to the United States with access to email using an iPhone. CAO and IT approved the travel.

Conditions

1. All devices are required to have a passcode and use encryption for passing of credentials to the server. Remote lock and wipe is available in case of breach or a lost device.

Reasons

1. Communication is required while travelling to keep in contact with key stakeholders.

Town of Mahone Bay

Description

1. Municipal property owners living outside of Canada are sent property tax invoices twice a year (April and July). There are sometimes email communications with these clients regarding their tax bills.

2. Customers of the municipal water and electric utility are sometimes sent information about their utility bills if they live outside of Canada or are vacationing outside of Canada. There are sometimes email communications with these clients regarding their tax bills.

3. One municipal elected official participated in an in-camera Council meeting via Skype.

Conditions

1. Email communication about personal information is initiated at the request and with the written consent the individual whom the information is about in accordance with Section 9(2)(b) of PIIDPA.

2. Email communication about personal information is initiated at the request and with the written consent the individual whom the information is about in accordance with Section 9(2)(b) of PIIDPA.

3. As is required of all municipal representatives who participate in in-camera meeting electronically, the elected official ensured that the room was cleared and used headphones to prevent meeting conversation from being overheard.

Reasons

1. The provision of information pertaining to tax bills is necessary for property owners to be able to pay their tax bills to the municipality.

2. The provision of information pertaining to utility bills is necessary for utility customers to be able to pay their bills to the municipality.

3. The elected official was participating in the meeting as part of fulfilling his responsibilities/requirements as an elected official.

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 using iPhone and iPads for Municipal Councillors, and both laptops and mobile devices for staff while travelling outside of Canada. 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 (10 unsuccessful 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 of stolen. No municipal data (outside of email) is stored on the mobile device, only accesses 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 serves 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 New Glasgow[21]

Description

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

2. In 2016, the New Glasgow Regional Police Service made the decision to utilize an Internet web based program 'Schedule Anywhere' for the scheduling of personnel of the New Glasgow Regional Police.

[21] This includes the New Glasgow Police Service.

Conditions

1. Mobile Devices have device password provisioned as well as securely managed and under the control of the Town's mobile device management software. Remote access for webmail includes encrypted communications with an SSL certificate and accounts are protected with usernames and passwords which are changed on regular basis. Laptop devices are configured with two-factor authenticated hard disk encryption and two-factor authenticated VPN access.

2. 'Schedule Anywhere' is maintained on a secure web site with SSL and is password protected. There are assigned administrators within Senior Management of the Police Service who assign permissions within the program.

Reasons

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

2. 'Schedule Anywhere' allows employees the ability to submit requests for time off electronically, and for the administrators/managers to approve time off requests electronically. 'Schedule Anywhere' also gives managers and supervisors the ability to view the status of resources/staffing electronically and improves the ability to allocate resources for deployment and training.

Town of Truro

Description

1. A number of Town of Truro employees (e.g., 9 employees) travelled outside of Canada with their Town issued smart phones. In each instance the employee requested and received approval from their supervisor and the CAO to take their device. The employees had access to the Town of Truro email system from their smart phone.

Conditions

1. All smart phones issued by the Town of Truro are required to have a passcode with a minimum of 6 characters. Remote access to the Town of Truro email server from mobile devices or webmail is secured by a signed SSL certificate.

Reasons

1. When Town of Truro staff or elected officials are travelling outside of Canada they are required to request and receive approval from their immediate supervisor in order to take with them any mobile devices owned by the Town. All requests approved by the supervisor are then reviewed by the CAO to determine if there is a necessity for the employee or official to travel with the device. Final approval by the CAO is required before devices are allowed to be taken out of country.

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. 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 (10 unsuccessful attempts). Access to municipal data on mobile devices outside of email is provided by the use of a VPN data connection. IT administrator can revoke VPN access should the mobile device be lost of stolen. No municipal data (outside of email) is stored on the mobile device, and accesses 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.

Town of Yarmouth

Description

1. Mayor, Council and staff have and require Remote Access to information while traveling outside of Canada. Staff and Council are provided remote access to email and staff are provided access to files stored at the Town of Yarmouth offices. Primary access to email is provided through the use of Web access to webmail for Town Councillors to access on their personal devices. Town staff are provided with mobile phones, tablets and/or laptops depending on their specific requirements.

Conditions

1. Mobile Devices: Access to email is provided via the internet (webmail).

   Access to municipal data on mobile devices outside of email is provided to staff by the use of a VPN data connection. 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, on accesses through the VPN connection. A passcode is required to access mobile devices.

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

Amherst Police Department, Annapolis Royal Police Department, Bridgewater Police Services, and Truro Police Service did not have access or storage outside of Canada to report.

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. Westville Police Department reported under Town of Westville. New Glasgow Police Service reported under the Town of New Glasgow.

Appendix 1

The following attachment was submitted by the Conseil Scolaire Acadien Provincial (see next page).

Assessment of a Proposed Digital Resource

The table below outlines the factors that Superintendents should consider when making decisions around the "necessity" of using a digital resource, web site or service that requires personal information to be disclosed, accessed or stored outside Canada.

Name of digital resource, web site, or service	Google Apps for Education
URL (if applicable)	http://www.google.ca/enterprise/apps/education
Name of person(s) proposing use of the digital resource, web site, or service	Nova Scotia school boards and schools

Factors	**School Board Response**
Describe the digital resource, web site, or service.	Google Apps for Education is a collection of online services (called "apps"). This assessment considers only Google's Core Services, specifically: • Drive (including Documents, Presentations, Spreadsheets, Forms and Drawings) • Sites • Gmail • Calendar • Groups • Contacts Any use of add-on apps or third-party apps would require further assessment.
Users and uses	
Who will be using the digital resource? How, or for what purpose, will they be using the digital resource?	Google Apps for Education would be used by students, teachers and administrative staff. Users may create and share documents, presentations, spreadsheets, forms and drawings, and store these and other files in an online storage space. Users may create and contribute to theme-based, domain exclusive web sites that can be shared with both internal and external users, as appropriate. The service can also provide a complete email, calendar

	and contacts function that can be configured for an educational domain of our choice e.g. NSPES.
Benefits	
What are the benefits of using the digital resource, web site or service? For example: Does it support learning outcomes, or goals of the school or school board? Does it assist with student, parent, or community engagement and/or discussion? How? Is it a free or low-cost service? Are there costs associated with the alternatives? (Note, the fact that a digital resource is free of charge is not sufficient to support the argument of "necessity". Cost cannot be the sole factor that determines "necessity".) Has a bias evaluation instrument been completed for this tool (for classroom resources), if applicable? If not applicable, please indicate the reason(s) it was not deemed necessary for this tool (e.g. the site is not content driven, users provide content so bias is not inherent to the site)	Google Apps for Education would support and encourage collaboration among teachers and students. The simplified, intuitive end user experience allows the focus to remain on the learning objectives, not the technology. 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. There is no license cost for the Core Services of Google Apps for Education. There will be some administration costs, however (e.g. maintaining user accounts, ensuring Internet and wireless access is robust). An evaluation of functional, technical and cost estimates was completed through the Regional Board Technology Supervisors. A bias evaluation has not been completed for this service, since the content is constructivist and therefore provided by students and teachers. There appears to be no obvious bias inherent to the toolset.
Equity	
How will equitable access be considered?	Additional access is provided anywhere, anytime through cloud based services. The choice of Google Apps for Education better addresses the trend of Bring Your Own Learning Tools and the wide variety of devices that are currently in the public school system. In addition, all students and teachers will have access to the same set of tools, and the latest version of the

	software. Software is updated automatically and available to everyone immediately, removing the current limitation of older versions of software in some schools or on some computers within the same school. Google Apps for Education does rely heavily on Internet (and potentially wireless) access. In that sense, there could be some disparity among schools with respect to infrastructure that may impact the end user experience.
Risks	
Is personal information collected by the digital resource? Is personal information required, such as student's full name, school, and grade? Is additional, more identifying personal information required, such as student's home address, phone number, or photo? Is there the option of providing only the minimum of information about a student or user, or are all fields required to be completed?	Google Apps for Education does collect personal information, in two senses. 1. **User-provided information:** Basic information is provided for each user in order to establish an account. This information is limited to first and last name, email address and encrypted password. Users may be able to provide additional information as they use the service (e.g. a photo). It is recommended that a student has a Personal Information Consent Form from the Network Access and Use policy signed, and parents/guardians have given permission for the school and board to publish student work and personal information as appropriate Schools should not post any additional personal information beyond what is noted in the consent form. Users may reveal personal information in other inadvertent ways as they use the productivity tools provided and store this in the cloud. In addition to the user-specific personal information, information about the board itself is provided when setting up Google Apps for Education, including: • The first and last name of the individual creating the account on behalf of the board • His/her email address and phone number (or a generic one) • The name of the board • The board website URL • The approximate number of students and staff (within a specified range)

	• The fact that the board is a primary/secondary educational institution • The fact that the board is Canadian While this information is not stored with the personal information of a specific user, the two could potentially be correlated. 2. **Google-collected information:** Google collects personal information as users use their services, such as device and software details, IP address, mobile phone number, location information, language, search history, and additional as indicated in the privacy policy link below. This information is generally used to monitor use and improve services, as well as customize content for the user (e.g. more relevant search results). As a result of a recent policy change, this information is no longer used for advertising purposes.
Evaluating the digital resource's Privacy Policy	
Is there a Privacy Policy? If yes, the following questions are suggested to help evaluate it: Is the Privacy Policy clear? Does it explain what personal information will be collected, how it is used and disclosed? Does it provide a method of reporting privacy breaches? Is personal information collected sold, shared, or otherwise released to other organizations or businesses? Are appropriate, industry-standard physical and technical safeguards used to	Google's privacy policy (http://www.google.com/policies/privacy/index.html) is quite clear, explains what information may be collected, and how that information may be used. There is no clear method of reporting privacy breaches, however. Google will not share personal information with third parties without user consent, except for legal reasons that include law enforcement, legal processes, enforceable government requests, potential violations of the Terms of Service, and security or technical issues as detailed. Google will notify customers as legally possible of any requests. Google uses industry-standard technologies and processes to safeguard user information, and maintains several third-party certifications with respect to security and privacy. Google clearly states that user data belongs to the user, not Google. Collected information is used for account creation, to provide, maintain, protect and improve the provided services, to develop new services, and to protect Google and its users. It is also used to offer users tailored

protect the web site and the associated information collected about users? Who owns the data that a user submits: the user or the digital resource, web site or service? How is unidentifiable information used? (E.g. web surfing habits, the ads visited, the pages opened, etc.)	content, such as more relevant search results. Email addresses may be used to contact users with service announcements.
Risk mitigation strategies	
Are there risk mitigation strategies in place to reduce risks to personal information?	The most effective mitigation to the risk of unauthorized disclosure of personal information is to limit the collection of that information. Google requires only minimal information in order to access and use the Core Services. Boards together with the EECD would need to establish policies and controls, as well as communicate best practices, to limit the amount of information students and staff might provide in addition to the minimum required. Examples include: • Educating students and staff about the risks of providing or storing personal information in a cloud service such as Google Apps for Education • Only using additional apps that have been approved • Establishing policies to periodically review user-provided personal information and take action to remedy any areas of concern • Establishing policies to discourage the use of these services for sensitive or confidential purposes • Establishing policies to periodically review any changes to Google's Privacy Policy and take action to mitigate any areas of concern Notwithstanding the above, users are able to add additional personal information, and as they use the services, will create additional personal information. Google provides the Google Dashboard (https://support.google.com/accounts/answer/162744) to allow users to see what information has been collected, and manage this information. Users should be encouraged to use this resource to manage their online identity.

Acceptable Alternatives	
Is there an acceptable alternative that does not require the access or storage of personal information outside Canada? Explain.	No alternatives were identified with data storage in Canada.
Other information relevant to the access or storage of personal information or proposed use of the digital resource Complete as necessary.	In addition to Google's Privacy Policy, the Terms of Service for Google Apps for Education (http://www.google.com/apps/intl/en/terms/education_terms.html) also has relevant implications: *"Google has implemented at least industry standard systems and procedures to ensure the security and confidentiality of Customer Data."* • User data can be expected to be at least as secure as it would be in any well-managed data centre. *"Google may transfer, store and process Customer Data in the United States or any other country in which Google or its agents maintain facilities."* • This is not unusual for cloud services, since one of the strengths of these services is the distribution of resources and resulting fault-tolerance. *"Google may make commercially reasonable changes to the URL Terms from time to time. If Google makes a material change to the URL Terms, Google will inform Customer by either sending an email to the Notification Email Address or alerting Customer via the Admin Console."* • Boards should implement a process to review and approve any changes to the Terms of Service for Google Apps for Education *"Google does not serve Ads in the Services or use Customer Data for Ads purposes."* • Boards can be confident, users will not be presented with ads as part of these services, nor will user data will be scanned for advertising purposes. *"Customer is responsible for responding to Third Party Requests."* • Google will not respond to a third-party request for access to information directly, unless bound

	by law to do so, but rather will inform the board administrator of the request so that the board may respond. *“Customer agrees that Google may include Customer's name or Brand Features in a list of Google customers, online or in promotional materials.”* • Google may use the boards’ names and logos for promotional purposes.