PERSONAL INFORMATION INTERNATIONAL DISCLOSURE PROTECTION ACT

2017 Annual Report

Nova Scotia Department of Justice

Message from the Minister of Justice

I am pleased to provide the twelfth 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, 2017 to December 31, 2017.

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.

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 February 1, 2018, a request was sent to public bodies[1] in Nova Scotia to complete and return a *PIIDPA* Form 1 for the 2017 reporting year by March 31, 2018. 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 2017 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 four (4) 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[3]

Description

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

2. V-LIMS (Veterinary Laboratory Information System) - See description of storage provided in the 2014 annual PIIDPA report under "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]The Department of Seniors, Elections Nova Scotia, and Public Service Commission did not have access or storage outside of Canada to report.

[3]The Department of Agriculture's PIIDPA Report also includes Agricultural Marshland Conservation Commission, Animal Cruelty Appeal Board, Atlantic Provinces Harness Racing Commission, Nova Scotia Crop and Livestock Insurance Arbitration Board, Nova Scotia Crop and Livestock Insurance Commission, Nova Scotia Farm Loan Board, Farm Practices Board, Farm Registration Appeal Committee, Livestock Health Services Board, Nova Scotia Natural Products Marketing Council, Nova Scotia Veterinary Medical Association Council and Weed Control Advisory Committee

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.

Business

Description

1. Two (2) employees travelled outside Canada and may have accessed personal information via their government issued electronic devices. Travelled destinations include: Ireland, USA

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 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. 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 with operations.

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 (GA) is the corporate standard for web analytics. Conditions or restrictions that have been placed on storage or access of personal information outside Canada include: Internet Protocol (IP) addresses will be 'marked', the last series of numbers in the IP address will be removed before being stored by GA, which reduces the ability to identify specific users; behavior on our websites. The GA software does not allow government staff access to individual IP addresses. Access to the analytics information will be controlled by password, and the information will only be presented in an aggregated form.

2. CNS is responsible for the government Twitter, Facebook, YouTube, Flickr, Tumblr, Instagram, and periscope accounts, which are based in the U.S. These accounts are used for sharing government news releases, videos, photos and other information to a broader audience.

3. Four employees of CNS travelled to the United States with mobile devices. Four employees also had a laptop.

Conditions

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

2. CNS uses social media platforms to share information and public engagement. No IP addresses are provided or collected. CNS retweets other government accounts and public safety information from partners (RCMP, Halifax Regional Municipality, etc.) CNS does not retweet personal accounts. Facebook shares are treated in the same manner.

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

Reasons

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

2. Social media platforms are used to increase public awareness and engagement, and to correct erroneous information. It is also used to monitor public opinion which helps government to make better informed decisions regarding policy, program and service delivery.

3. BlackBerrys and iPhones 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[4]

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 over the past 2 years. Nova Scotia Provincial Library manages the account with the vendor RB Digital (formerly Zinio) on behalf of four regional public libraries. The decision to use the RBDigital for libraries platform was made because there was no Canadian company that is as robust as RBDigital in terms of development, or content. Users share their library card number, first and last name and their email address with RBDigital to create their account. Other information is automatically

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

collected based on how the user interacts with the system. RBDigital'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. Ebook access (elending) has quickly become a critical service that libraries provide to clients. A technical change made by our existing service provider (OverDrive) in 2015 led to the storage of the personal information of libraries users on servers outside of Canada (previously, it authenticated against our locally-housed database). The OverDrive platform, used by libraries to circulate digital materials (primarily ebooks and audiobooks) to library users, has changed from using Adobe IDs to enforce the Digital Rights Management (DRM) applied to individual titles, to an account-based model. New users are required, and most existing users, will need to create OverDrive accounts to improve user experience and eliminate usage barriers. New OverDrive accounts contain personal information about identifiable individuals (library clients in Nova Scotia), including name, email address and/or facebook information. This personal information is voluntarily provided when a client registers for the OverDrive service. OverDrive collects certain information about client interactions with them and information related to clients and their use of the service, including but not limited to, personal information, system activity, digital content selections, reviews and ratings, as well as Internet Protocol addresses, device types, unique device data, such as device identifiers, and operating systems.

4. Continued use of Social Media Accounts (Twitter, Facebook, lnstagram, YouTube and Flickr)
    a. Twitter: @NS_Museum, @MNH_Naturalists, @NS_MMA,@FisheriesMuseum, @RossFarmMuseum, @McCullochHouse, @Highlandv, @Sherbrooke_NS, @fundygeo, @uniackeestate, @ns_moi, @FFmuseumofNS, @SailBluenosell, @OfficeofANSA, @NovaScotia, @GouvNE, @NS_CCH, @NS_Archives.
    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, lomairtean na Gaidhlig/Gaelic Affairs, Nova Scotia Provincial Libraries.
    c. lnstagram: @rossfarmmuseum, @highland_village, firefighters_museum_of_ns, @fisheriesmuseum, @novascotiamuseum, @mnhnovascotia, @ns_mma,

@uniackeestatemuseum,@blackloyalistheritagecentre, @villageacadien, @ns_archives.

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.
f. Nova Scotia Archives Pinterest Board.

5. Remote access via electronic devices such as BlackBerrys, 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. RBDigital 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. The vendor is in the process of implementing protocols that will ensure the product is compliant with the EU's General Data Protection Regulation (GDPR) in accordance with the May 25, 2018 deadline.

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 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. Efforts were made to ensure that Privacy information was readily accessible to service users. The OverDrive privacy policy and terms and conditions clearly state what personal information is collected, the information that can be associated with users and the ability for users to opt out of data collection metrics. There is also the ability for individuals to clear their borrowing history and delete associated cookies from devices. The vendor is in the process of implementing protocols that will ensure the product is compliant with the EU's General Data Protection Regulation (GDPR) in accordance with the May 25, 2018 deadline.

4. N/A

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

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

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

Community Services[5]

Description

1. Eighteen (18) staff members travelled outside of Canada in the 2017 calendar year with government devices.

Conditions

1. Devices were password protected.

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 they were out of the country.

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

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. Scratch - Scratch is used by students and their teachers worldwide to program their own

interactive stories, games, and animations, and share their creations with others in an online community. Scratch is a project of the MIT Media Lab and originates from the United States. It can be used for a range of educational purposes from science and mathematics projects, including simulations and visualizations of investigations, recordings, and interactive art and music. Personal information about students and teachers will be accessed and stored outside Canada as the Scratch server is located outside Canada.

9. Social Media - The Department operates a Twitter account. Twitter is based in the United States. This account is used for sharing government news releases, videos, photos and other information to a broader audience.

10. 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.

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

Conditions

1. Provincial Student Information System - The Department of Education and Early Childhood Development has implemented reasonable security measures to protect electronic storage of personal and other information in the SIS. The information and software are maintained in a secure environment. The contract with the service provider stipulates that Department of Education and Early Childhood Development staff will authorize access to the environment to the PowerSchool Group, 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. TIENET - The Department of Education and Early Childhood Development has implemented reasonable security measures to protect electronic storage of personal and other information in the Extended Services and Programming system. The information and software are maintained in a secure environment. The contract with the service provider 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. Teacher Certification Fee Processing - The Online Payment System has been developed in adherence with government and departmental security standards to ensure system access is

restricted to authorized individuals and information is protected against unauthorized disclosure. Cardholders have agreed to the card issuing institutions' privacy statements that include a notice that third party service providers may be used to process credit card transactions.

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

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

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

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

8. Scratch – At school, devices are subject to Internet security provided. All devices and their use are subject to the Network Access and Use Policy. Scratch has physical and electronic procedures to protect the information that is collected. They strictly limit individual access to the Scratch servers and the data they store on them.

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

10. Smartsheet - 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.

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

Reasons

1. Provincial Student Information System - The decision to contract with 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. TIENET - 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 Fee Processing - Teacher Certification offers the option of payment by credit card payments as a convenience for teachers, and to provide efficient and effective online services.

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

5. Correspondence Study Program Payment Service - The option of payment by credit card is a convenience for students, and provides efficient and effective online services.

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

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

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

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

10. Smartsheet - 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.

11. 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 access email and Internet sites, and make telephone calls. Laptops etc. are needed for preparing documents, and accessing email and Internet sites.

Energy

Description

1. Five members of the Department of Energy were authorized for personal travel outside of Canada in seven instances to carry their government issued mobile phone and/or computer in order to ensure business continuity. Additionally, 11 staff travelled for business outside of Canada on 28 occasions to eight 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.

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.

Environment

Description

1. There were 11 instances of travel to countries outside Canada taken by Nova Scotia Environment staff in 2017. In each case, staff received approval from the Deputy Minister to take their electronic devices.

Conditions

1. Remote access to information on electronic devices is protected by username and 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 reasons. Therefore, they may require access to email and other government records.

Executive Council[6]

Description

1. Seven (7) employees traveled outside of Canada on eight (8) different trips. All seven employees took their BlackBerrys or iPhone and one took a BlackBerry and a laptop. These employees traveled to various states in the United States of America and Europe. Five employees had permission from the Clerk of the Executive Council to travel with the device. One employee crossed the border between Canada and the USA for twenty minutes with her work iPhone in her belongings. One employee travelled to the USA for both work and personal reasons and forgot to request permission to take his BlackBerry. The Deputy retroactively gave permission for both employees to have taken these devices to the USA. No privacy breaches resulted from these two incidents.

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 includes transport of personal information in a cell phone or other electronic device (e.g. a BlackBerry, iPhone, or iPad). Also under PIIDPA, storage or access of personal information outside of Canada may be permitted by the Deputy Head if the Deputy Head considers that the storage or access is necessary to meet the requirements of the department's operation. Permission must be sought from the Deputy Head for transport and, as necessary, the storage or access of personal information while outside Canada.

Finance and Treasury Board

Description

1. Between January 1, 2017 to December 31, 2017 five (5) staff members were granted approval to travel outside Canada with mobile devices and therefore had the ability to access personal information via email or in documents if saved on those devices.

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.

[6] On September 21, 2017 Order in Council 2017-234 created the Office of Strategy Management (OSM). For the purpose of this report employee activities of OSM are reporting through the Executive Council Office.

Reasons

1. Staff may be required to monitor their email and voicemail for business continuity purposes. Mobile 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.

Fisheries and Aquaculture[7]

Description

1. Remote access via electronic devices such as BlackBerrys, laptops, and tablets - There were 29 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 "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

1. En-Pro Automatic External Defibrillator (AED) Registry - En-Pro Inc. will provide a registry of record for Automatic External Defibrillator (AED) placements within the province of Nova Scotia. The data contained in the registry is under the custody and control of EHS and will be used for mapping resources to anticipated patient volume demand. En-Pro Inc. will provide periodic notification to the Province of new AED registrations no less than quarterly, maintain the Registry free of charge for organization and AED registrants. protect registrants' privacy and not use, sell or otherwise divulge any ownership or location information to any commercial entity, and provide reminders to replace electrode pads and/or batteries when necessary. Personal health information will not be collected. Only the agency/AED registrant contact and

[7] Fisheries and Aquaculture's PIIDPA report also includes Nova Scotia Aquaculture Review Board, and Nova Scotia Fisheries and Aquaculture Loan Board

volunteer information will be collected with express consent. En-Pro Management Inc. is a subsidiary of ZOLL Medical Corporation, 9242 Ellerbe Rd., Suite 300, Shreveport, Louisiana, 711 06.

2. 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 Jog 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.

3. 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 Naida, 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.

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

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. 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.

8. DHW Employee Access - Between January 1, 2017 to December 31, 2017 one (1) staff of the Department Health and Wellness was granted approval to travel outside Canada on business with mobile devices and therefore had the ability to access personal information via email or in documents if saved on those devices (e.g., downloading PDFs to read on device).

Conditions

1. En-Pro Automatic External Defibrillator (AED) Registry -The information captured in the AED registry will be stored on DOD Tier Ill servers, the highest level of security available as designated by the U.S. Department of Defense, and is not available in paper form. The information is controlled by permissions only granted to users within Nova Scotia. Administrative control is provided by the En-Pro Manage customer service team in Shreveport, LA. No information at any time can be downloaded or stored on portable devices. The En-Pro data center is SSAE SOCII (formerly known as SAS 70 Type II) compliant. The facility maintains 24x7x365 staffing of security and Network Operations Center personnel, monitoring, video surveillance, biometric and access card with mantrap access to the data center floor. Physical access to the servers is limited to authorized personnel only, who are allowed entry with proper photo identification, an iris scan, and escort of a staff member. Upon entry to the facility, visitors must sign in at the security desk and surrender a valid TSA-approved ID to obtain a visitor's pass. Its servers are protected by a Cisco ASA 55 10 firewall to prevent unauthorized access. Pingdom, a third-party service, is used to notify ZOLL employees if the SSL Certified PlusTrac website becomes unavailable.

2. 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. HlPAA is United States federal law which includes provisions for the protection of privacy of certain individually identifiable health information referred to as protected health information.

3. 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 (PH/A).*

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 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 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. Panorama, IBM Canada Ltd. - The Master Services Agreement between IBM and the Province (DHW and lSD) includes Schedule 15 Privacy and Security Obligations which defines the conditions under which access is provided for out-of-country technical support. Data will be stored to data centers within Canada. 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.

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. En-Pro Automatic External Defibrillator (AED) Registry - The EHS Public Access Defibrillation (PAD) Program achieves the clinical care standard expected per national and international published guidelines for improving the survivability from out of hospital cardiac arrests. EHS shall establish the standards of care for bystander CPR and AED usage, the associated performance measures and benchmarks, and the resultant quality improvement system. Moreover, it will assume a leadership role in any associated program evaluation and/or research in compliance with all associated ethical and privacy standards within the province. EMC shall provide all operational aspects of public AED Identification, registration, communication, and enrolment into the PAD Program and operational aspects of the En-Pro Inc. system within the existing high performance contract requirements in the Ground Ambulance, Medical First Responder and Medical Communications Centre. This will be in parallel to the existing monitor therapeutic system and ePCR system of care. The chosen product (Atrus AED Link) is specialized software first discovered and explored by EHS and EMC back in 2013. Providers of such specialized software are very limited to the market and to EMC's knowledge there were no known Canadian software companies *I* vendors providing such software solutions at the time of purchase. The Atrus AED Link allows for an electronic registry of AED placements throughout Nova Scotia which will support improved responsiveness and effectiveness for public safety.

2. FairWarnlng - The FairWarning application is used to augment 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 is used to augment current user access audit approaches for various provincial health information systems.

3. 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.

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 Healthlink 811 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. 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. The intended scope of the Panorama Implementation Project includes Vaccine Inventory, Immunization, and Communicable Disease Investigation and Outbreak Management. 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.

8. DHW Employee Access - When staff are traveling for business reasons (e.g. meetings, conferences) they are expected to monitor their e-mail and voice mail where possible. Therefore, it is necessary for them to check e-mail remotely where possible to fulfill their responsibilities. As per PIIDPA, any employees that meet this need must submit their request for approval by the Deputy Minister of Health and Wellness.

Intergovernmental Affairs

Description

1. Remote access via electronic devices such as BlackBerrys, laptops, and tablets. There were twenty-five (25) 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.

Internal Services

Description

1. Travel outside of Canada with Electronic Devices: Thirty-nine (39) 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, iPhone, 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 Forty-three (43) business trips outside of the country in 2017 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 was previously stored in Chicago in the USA and is now housed in the United Kingdom. The system will be executed remotely by I RM 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 below, 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 SystemTangoe 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 Feb 2013 to Jan 2016 was extended to March 2021.

8. Yammer Enterprise Social Network: Yammer is an integrated Enterprise Social Network component of Office 365. Unlike other components of Office 365 the data for Yammer is not able to be hosted within Canada. Yammer is a tool for NS Government employees to share information and engage with each other. This NS Government instance of Yammer was initialized in November of 2017 as a part of the rollout of the full Office 365 software suite. Yammer collects the email address, and any content the user elects to share.

9. Eventbrite Event Registration: To allow staff to register for Employee Engagement Week (June 12-16, 2017) Eventbrite was selected as service. Eventbrite operates out of San Francisco, California, USA. The service collected the name and email address of provincial government employees who elected to register for the event. Eventbrite's privacy policy indicates that personal data may be stored by third parties.

Conditions

1. Staff use of government-issued BlackBerry or iPhone 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. This information is subject to the Pictometry Privacy Policy.

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

5. 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. 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. 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.

8. Use of Yammer is subject to guidelines including the Nova Scotia Public Service Code of Ethics, Respectful Workplace Policy and Social Media Policy.

9. This information is subject to the Eventbirte Privacy Policy and Terms of Service. Employees were able to register by emailing the event organizer as an alternative to using the Eventbrite site.

Reasons

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

2. This allows the province to access oblique photographs to align with Municipal Partners

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

4. Risk Management and Security Services - After reviewing the Province's business requirement, IT Management recommended implementation of ASP Stars as it fit the operational requirements of the Risk Management and Security Group and there wasn't a cost effective Canadian solution available. The STARS system has been in operational use by Government for 18 years. The information contained is common to information found in normal search of personal information such as name, address and phone number. Only the section of STARS dedicated to Occupational Health & Safety contains medical cause and treatment information.

5. 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. 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. 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 US requires that information flows through an Automated Clearing House. There is no ACH that stores information in Canada.

8. As a part of our implementation of Office 365, Yammer allows NS Government Staff to engage with each other in a Social Network environment while allowing a greater level of control of access than using public Social Networks like Facebook or Twitter.

9. A registration service was required to manage the attendance of staff for Employee Engagement Week Events. Canadian hosted alternatives were cost prohibitive for this initiative so Eventbrite was chosen with an alternative option for those who did not wish to use the service.

Justice[8]

Description

1. Twenty-two Employees Traveled outside of country with a BlackBerry or laptop that contained personal information or could access personal information.

2. In 2016, the JEMTEM Inc. 2008 contract for Electronic Supervision of Offenders was renewed.

3. The Director of MEP has an obligation, pursuant to the Maintenance Enforcement Act, to enforce all maintenance or support orders which have been filed for enforcement with the Director, including outside of Canada.

4. 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.

5. In July 2004, the Department of Justice entered into a service contract with Iron Mountain Canada Corporation to provide document destruction and government record storage. This contract ended on March 31, 2017 and all Justice boxes have been removed from Iron Mountain to be stored in a Government owned facility.

Conditions

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

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

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

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

4. The particulars about the 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. 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. Permission to take BlackBerry out of the country was granted to allow contact with staff and to deal with matters or urgent issues while travelling.

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

3. The particulars about the 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.

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

5. The particulars about the 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) has a Memorandum of Understanding with GED® Testing Service LLC for the administration of the GED® testing program in Nova Scotia. 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® 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 and ensuring compliance of test administration. GED® testing is administered by 40 states in America and the Canadian provinces and territories, with the exception of British Columbia. 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 GED® Testing Service is based in Washington, D.C. with additional offices in Minneapolis, Minnesota. GED® Testing is completed on-line (at GED® testing Centers across the province), except in select federal & provincial correctional facilities where paper-based testing is still offered. The website GED.com, and within that webpage, GED® Manager, is utilized for the purpose of storing and processing tester (student) information

and results, in support of the GED® testing program. The individual tester registers directly through GED.com for testing.

2. There were sixteen (16) employees, in twenty-one (21) instances, who traveled outside Canada with a mobile electronic device, such as a BlackBerry or cellphone, that contained personal information or may have been used to access personal information.

Conditions

1. The individual tester upon registration on GED.com must agree to the GED® Test Non-Disclosure Agreement. The agreement outlines the use of the testers personal information by GED® Testing Service LLC.

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. All devices are password protected.

Reasons

1. GED® Testing Service LLC is the sole source provider of the GED® testing program. In 2014, LAE changed service providers from NRSPro to GED® Testing Service LLC as the testing changed to the computer-based format and there was no use for NRSPro's service. At that time, Nova Scotia's data was transferred to GED® Testing Service LLC. At the present time, there is no option of a software solution with data storage in Canada.

2. When staff are traveling 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) staff travelled outside of Canada on business/pleasure and took either their cell phones or laptops with them.

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 and 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.

Natural Resources

Description

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

Conditions

1. Permission must be granted in order to take an electronic device out of the country. Remote access to email is protected by username/password authentications and is delivered over a secure server link (SSL) encrypted link. All government issued electronic devices must be password protected.

Reasons

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

Office of the Premier

Description

1. Seven (7) employees traveled outside of Canada on 18 different trips. All seven employees took their BlackBerrys/iPhones and one took a BlackBerry and a laptop. The employees traveled to various states in the United States of America, Aruba, and Europe. All seven employees had permission from the Chief of Staff, Office of the Premier 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, iPhone 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 iPhones, BlackBerrys, laptops, and tablets. There were nineteen (19) instances in which staff members were approved to take electronic devices while travelling outside Canada and may have accessed personal information, such as that contained in email. In two (2) instances, staff members travelled with their electronic devices outside of Canada without first seeking authorization to do so.

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. The employees involved in travelling without authorization have received training on PIIDPA requirements.

Reasons

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

Public Prosecution Service

Description

1. There was no storage of personal information outside Canada by the Public Prosecution Service. There was access to personal information using iPhone by eight individuals while traveling outside Canada.

Conditions

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

Reasons

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

Tourism Nova Scotia

Description

1. Remote access via electronic devices such as BlackBerrys, laptops, and tablets. There were 28 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 MailChimp. 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. MailChip: see description of reasons provided in the 2013 annual PIIDPA report.

Transportation and Infrastructure Renewal

Description

1. There were 54 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 2017. One travelled to Europe, one to the Czech Republic, two to the Caribbean, one to New Zealand, one to China and South Korea, two to Mexico, and 46 to United States. BlackBerrys 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. FY 13/14 it was confirmed that only IRP jurisdictional staff have access to this information which is password protected on a secure web site.

Service Nova Scotia[9]

Description

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

2. 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.

3. Five SNS staff traveled outside Canada during the reporting period on nine separate occasions. One staff member travelled five times. SNS staff took their laptop and/or mobile device phone with them while out of the country.

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.

Conditions

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

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

2. 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.

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

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

2. 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). SNS has an incremental STOR development project underway that will allow it to begin dispositioning and transferring some of its records to the Provincial Records Centre (subject to space availability). Until SNS completes that project 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.

3. Maintain contact with operations.

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[10, 11]

Atlantic Lottery Corporation

Description

1. **E-mail, storage and collaboration** - Employees of AL use Microsoft Office 365 for e-mail, storage (OneDrive) and collaboration (SharePoint). As of November 2017, all of ALS core data including e-mail, storage and collaboration data reside within Microsoft's Canadian datacenters. Due to the nature of the O365 platform and that many of its secondary services operate solely within American datacenters, it is possible for personal information to inadvertently be stored on those servers for the duration of time determined by the secondary services.

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 Bitlocker with AES 256-bit encryption on servers that hold all messaging data, including email and IM conversations, as well as content stored in SharePoint 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 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.

---

[10] The Human Rights Commission, Nova Scotia Legal Aid Commission, Nova Scotia Public Service LTD Plan, Office of the Police Complaints Commissioner, the Nova Scotia Provincial Lotteries and Casino Corporation, and Workers' Compensation Appeals Tribunal did not have access or storage outside of Canada to report.

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

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 access email and Internet sites, and make telephone calls. Laptops and iPads are needed for preparing documents, and accessing email and Internet sites.

Divert NS

Description

1. Our website, dlvertns.ca is now hosted outside of Canada. From May 2016 to Dec 2017 we used a Canadian hosting service, but it was unstable (continually crashed) and was too slow for users outside the Halifax region. It no longer met our requirements:
    - Live within a managed VPS environment or higher to meet our security and stability needs
    - Meet a high level of reliability and uptime
    - Respond to user browsing and Interaction within standard time expectations (< 2 seconds for server response, preferably lower).

    We switched to a US host in December 2017 that met our needs as above.

Conditions

1. The only personal information collected via our website is: name, email and postal code. This is collected specifically for public contests we run two to three times per year. Contests last approximately 2-3 weeks and once they end, we download the contest entrants' information onto our servers (hosted in Canada) and delete the Information from our website. The submitted Information is only accessible on the backend of our website via our CMS. Users require a password and username to access our CMS. The new host is class-leading in terms of security, reliability and speed. Website data is stored in the US, in a secure database in a custom-tailored and standalone environment. Access credentials for the database are stored solely within Canadian offices and are protected within an encrypted database.

Reasons

1. Divert NS requires a website to provide information and interact with Nova Scotia residents and our stakeholders. As mentioned above, we tried to use Canadian hosting services, but it was unstable, too slow and unreliable. We took steps to investigate other service providers (Including other Canadian options), and determined the best option to meet our functional needs was a US host, and we selected the one that offered the best security services.

Halifax Harbour Bridges[12]

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. There were 12 instances of employees travelling for business or work with their laptop or other electronic devices.

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. 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. 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.

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 Compliant, SSAE-16 compliant (formerly SAS70), 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. Recently, HHB implemented two-factor authentication which adds another layer of security beyond the password and deters potential hackers by making it difficult for them to access important information.

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

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

4. N/A

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.

4. N/A

Innovacorp

Description

1. SurveyMonkey - Is an online survey development cloud-based software. 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.

2. Doodle – Is a web-based scheduling tool that eliminates the hassle of organizing meetings via email or phone. Data collected includes name, email addresses and information related to the meeting.

3. Nexudus – Allows employees and clients to book resources and check availability online and allows Innovacorp to charge clients based on the resources booked and length of booking. Data collected includes name, email address and password.

4. Slack – Unifies employee communications through instant messaging. Discussions are organized into channels, so there's a place for every project, team or department.

5. Social Media – Innovacorp has Twitter, Facebook and Instagram accounts which are based outside of Canada. These accounts are used for sharing news releases, videos, photos and other relevant information. No IP address or personal information is collected through these services.

6. Employee Travel - Innovacorp employees accessed information using their mobile phones and/or computers while travelling outside Canada a total of 23 different times during 2017.

Conditions

1. SurveyMonkey – The storage and access of anonymous employee and/or client survey data is to be protected in accordance with the SurveyMonkey's terms of service.

2. Doodle - In accordance with their privacy policy, Doodle only shares information with the consent of the user. Doodle does not sell its data to third parties.

3. Nexudus – In accordance with their privacy policy, Nexudus does not provide its clients' information to third parties.

4. Slack – In accordance with their privacy policy, Slack only shares information with third parties with the consent of their client.

5. Social Media – Innovacorp uses social media platforms to share information and engage the start-up ecosystem.

6. Employee Travel - Information stored in or accessed by an Innovacorp director, officer or employee during international travel is to have a reasonable and direct connection to the person's job duties and be protected by the director, officer or employee in accordance with Innovacorp's Code of Conduct and Innovacorp's Information Technology Policy.

Reasons

1. SurveyMonkey – Domestic suppliers do not currently meet Innovacorp's technical and service requirements.

2. Doodle – Domestic suppliers do not currently meet Innovacorp's technical and service requirements.

3. Nexudus – Domestic suppliers do not currently meet Innovacorp's technical and service requirements.

4. Slack – Domestic suppliers do not currently meet Innovacorp's technical and service requriements.

5. Social Media – Platforms are used to increase public awareness and engage the start-up ecosystem.

6. Employee travel - For business continuity purposes, Innovacorp directors, officers, and employees must be able to store and access 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. – CRM data services – storage and access – client/partner/service provider representatives' personal information (primarily business contact information). Pursuant to s. 5(2) PIIDPA the head of Nova Scotia Business Inc. (NSBI) determined the

storage/access outside Canada of individuals' business contact information in NSBI's custody/control, as part of customer relationship management (CRM) data services supplied under contract by salesforce.com, Inc. (a Delaware, US corporation with its principal place of business in San Francisco, California) is to meet the necessary requirements of NSBI's operation.

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

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

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

5. Form Assembly – Online collection of information related to program applications and surveys – business contact information. Pursuant to s. 5(2) PIIDPA the head of Nova Scotia Business Inc. (NSBI) determined the storage / access outside Canada of individuals' business contact information (primarily e-mail addresses, names and titles) in NSBI's custody/control, as part of online form development management services supplied under contract by Form Assembly (a US corporation with its principal place of business in Bloomington, Indiana) is to meet the necessary requirements of NSBI's operation.

6. NSBI directors, officers, employees – performance of duties during international travel – storage and access – personal information. Pursuant to s. 5(2) PIIDPA the head of NSBI determined the storage/access outside Canada of personal information in NSBI's custody/control, stored in, or accessed using, a mobile electronic device by an NSBI director, officer or employee for business continuity purposes during international travel, is to meet the necessary requirements of NSBI's operation. There were Forty-eight (48) 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 165 trips taken in 2017.

7. PayPal Canada – PCI compliant payment platform/gateway collecting monies owed for participation in NSBI lead events and missions. Business contact information, credit card information disclosed directly to PayPal and not in NSBI's custody. 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, credit card information and telephone number (provided by the individual not disclosed to or by NSBI) as part of online payment platform process provided by PayPal Canada (a US corporation with its corporate headquarters in San Jose, California) is to meet the necessary requirements of NSBI's operation.

Conditions

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

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

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

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

5. Form Assembly – Online collection of information related to program applications and surveys – business contact information. Information collected during the application for programs, completion of surveys, and collection of business information is passed through Form Assembly servers and rests in Salesforce or Form Assembly and used by NSBI employees in aggregate or individually to process applications, measure program delivery.

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

7. PayPal Canada - PCI compliant payment platform/gateway collecting monies owed for participation in NSBI lead events and missions. Business contact information, credit card

information disclosed directly to PayPal and not in NSBI's custody. Through the payment process for events, missions and programs, clients provide their personal information diretly to PayPal Canada (US-based data centres) pursuant to PIIDPA Section 9(b) after agreeing to the terms and conditions of the events registration application and privacy statement indicating the information will be collected and stored outside of Canada. The information provided to PayPal is not ever in the custody of NSBI but this step is required to register for paid events.

Reasons

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

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

3. Proposify (PitchPerfect Software, Inc.) – sales proposal management services – storage and access – prospective client representative's business contact information (name, e-mail address) and proposal interaction analytics (after March 31, 2015)NSBI requires a convenient and secure proposal management service for streamlining the creation, management, customization of NSBI sales proposals, value proposition and program / service promotional presentations for prospective business clients, that can be integrated with NSBI's Salesforce.com CRM service.

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

5. Form Assembly – Online collection of information related to program applications and surveys – business contact information. The ability to streamline the collection of information from clients for program applications, surveys, and business contact information updates in our CRM system (Salesforce) requires modern and convenient methods that reduce the administrative time and data entry errors. Form Assembly offers deep integration with Salesforce and the ability to make complex forms without the need for programming or development. We will be

changing to keep our data on Canadian servers after March 31, 2018. We also have the ability to purge information from Form Assembly servers once it is posted to Salesforce.

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

7. PayPal Canada - PCI compliant payment platform/gateway collecting monies owed for participation in NSBI lead events and missions. Business contact information, credit card information disclosed directly to PayPal and not in NSBI's custody. In accordance with the Province's PCI compliance policy, a PCI compliant solution is required for collecting monies owning from clients through the course of registering for NSBI events, missions and programs. Through consultation with Service Nova Scotia, it was deemed the volume of transactions did not warrant the use of the ACOL payment system and the costs and priority of setting this up was prohibitive to the continuity of business. The PayPal Canada solution was established as an alternative solution until such time Service Nova Scotia offered a GPSLite solution for payment collection.

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 Liquor Corporation

Description

1. In 2017, the NSLC opened an account with Eventbrite, as an 'organizer', to support online ticket sales for events at The Port by the NSLC. Tickets for events were available for purchase in-store as well as online through Eventbrite. This option was pursued because of the convenience it offers NSLC customers. This service allows the NSLC to communicate with the ticket holders in the circumstance that an event needs to be cancelled, postponed or adjusted. This service also allows the NSLC to more easily manage inventory. Other benefits are:
    - Offers convenient way for NSLC customers to purchase tickets and to easily access their online order if they lose their physical ticket
    - Seamlessly integrate with the NSLC's website and social media channels
    - Track analysis to determine opportunities to improve NSLC events

- Remind ticket holders of their upcoming events

Personal information collected by Eventbrite is stored in the United States. The NSLC completed a Privacy Impact Analysis to understand the applicable legislation and to confirm Eventbrite had the necessary safeguards in place to protect any personal information provided by NSLC customers required to purchase an event ticket.

2. In 2017, the NSLC identified one business need addressed by the Office 365 project is the desire to move from NSLC on-premise access of information to mobile access, anytime and anywhere. Currently, NSLC employees have access to information within the NSLC offices or outside of the NSLC offices through a VPN connection. Moving to Microsoft Online Services will extend the availability of information to employees on most popular devices (e.g. smartphones and tablets). Another need was the ability to address the broken features from the existing Intranet (Swizzle) SharePoint 2013 site, which has become an important business tool. The existing Swizzle site has custom built web parts and design, which are affecting performance and causing functionality issues. The content migration to SharePoint Online will provide the Swizzle site with the flexibility and capability to support further development of Swizzle initiatives without the need to take on additional migration projects. Features are pushed to the cloud by Microsoft as they become available. To support the connectivity to Microsoft 365 services, the NSLC must synchronize their Active Directory with Azure AD Connect, which is stored in the United States. Azure AD Connect Synchronization (red line) synchronizes the NSLC Active Directory employee data with Azure AD and also maintains synchronization with the Azure AD Connect Staging server located in the Disaster Recovery site. The synchronization of data occurs on a regular-timed schedule (e.g. every 15 minutes). Synchronization between NSLC Active Directory and Azure AD provides employees with a single identity for using Office 365, Azure and SaaS (Software as a Service) applications integrated with Azure AD. Azure AD Connect Staging is not Active and will only be switched to Active status in the event of an outage with Azure AD Connect at the Head Office location.

3. Information was accessed by NSLC employees during business & personal travel. Devices such as phones, tablets and computers were used. Fourteen employees traveled during this time and information was accessed from the US, Spain, Jamaica, Mexico, Norway, Ireland, Italy, France, United Kingdom, Bahamas, Saint Martin, Bermuda and Portugal.

Conditions

1. Through the Privacy Impact Analysis, the NSLC is satisfied that Eventbrite has the necessary privacy and security safeguards in place. Eventbrite Security and Safety Guide identifies the following:
    - All Eventbrite employees are subject to reference, education and other personnel checks. Certain employees are also subject to detailed background checks
    - Eventbrite maintains an information security training program that meets PCI-DSS standards
    - Knowledgeable full-time security personnel are on staff
    - Eventbrite requires written acknowledgement by employees of their roles and responsibilities with respect to protecting user data and privacy.

    Eventbrite's Privacy Policy indicates that it has security measures in place to protect the personal information it holds from unauthorized use, access, disclosure, distribution, loss or alteration. Access to personal information is restricted to their authorized personnel who require the information to perform their jobs. Access to personal information by authorized personnel is further restricted to that which is strictly necessary for the performance of those duties. Eventbrite's European (EU) Data Protection guide provides details on Eventbrite's role and how it meets its data protection obligations for personal information.

2. Microsoft will only use customer data to provide the services agreed upon, and does not mine it for marketing or advertising. Customer data is stored in the agreed upon geographic location. Microsoft also complies with international data protection laws regarding transfers of customer data across borders. Microsoft takes strong measures to protect customer data from inappropriate access, including limits for Microsoft personnel and subcontractors. Microsoft does not give any third party (including law enforcement, other government entity, or civil litigant) direct or unfettered access to customer data except as directed by the customer. Microsoft does not provide any government with their encryption keys or the ability to break their encryption. Microsoft protects intellectual property and takes claims of copyright infringement seriously. Microsoft Security Incident and Breach Protocol-Microsoft has a global, 24/7 incident response service to mitigate the effects of any attacks or malicious activity. In the event of a security incident, Microsoft's policy is to promptly (i) notify NSLC of the incident; (ii) investigate the incident and provide the NSLC with detailed information about the incident; and (iii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the incident. Notification(s) are to be delivered to one or more of NSLC's administrators by any means Microsoft selects, including email. NSLC is required to notify Microsoft promptly about any possible misuse of accounts or authentication credentials or any security incident related to an online service offered under Office 365. Microsoft Azure uses virtual networking to isolate NSLC's traffic from other tenants, employing measures such as host- and guest-level firewalls, IP packet filtering, port blocking, and HTTPS endpoints. However, most of Azure's internal communications, including infrastructure-to-infrastructure and infrastructure-to NSLC (on-premises), are also encrypted. For communications within an Azure datacenter, Microsoft manages networks to assure that no VM can impersonate or eavesdrop on the IP address of another.

3. 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. The NSLC completed a Privacy Impact Analysis to understand the applicable legislation and to confirm Eventbrite had the necessary safeguards in place to protect any personal information provided by NSLC customers required to purchase an event ticket. Through the Privacy Impact Analysis, the NSLC is satisfied that Eventbrite has the necessary privacy and security safeguards in place.

2. Meets all necessary requirements.

3. Meets all necessary requirements.

Nova Scotia Utility and Review Board

Description

1. 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 (BlackBerry or Computer) - There were six (6) instances of employees traveling outside of Canada with the ability to access

personal information on a device or through a secure portal into the Board's internal network via mobile device or remote access.

Conditions

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

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

2. 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.

Nova Scotia Municipal Finance Corporation

Description

1. Two instances in which an employee travelled outside of Canada with their cell phone.

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 the country is in accordance with the standard provincial authorization process relating to international travel and provincially provided communication devices.

Securities Commission

Description

1. There were 18 instances where staff members were approved to take their BlackBerry or other electronic device while travelling outside Canada. Of these 18 instances, one staff member cancelled their trip prior to travel and, therefore, only 17 instances of the approvals were utilized. Staff members may have accessed personal information while travelling outside Canada with their approved BlackBerry or other electronic device.

Conditions

1. Permission must be granted 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.

Events East[13]

Description

1. The ticketing system used by Ticket Atlantic is hosted in Irvine California. USA by Paciolan. LLC. The data is housed in their managed facility on their AS6000 mainframe computers. Secure access is provided from Events East 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 Events East.

2. The online survey program used by Events East 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 Events East.

Conditions

1. Only Ticket Atlantic employees and agents can access the information through the secured VPN tunnel. Our contract states that Paciolan, LLC. will only use the collected customer information "solely for the purposes contemplated in this agreement and otherwise in compliance with all applicable federal and state laws. (The) Customer will own all Personal Information, data and related information collected or received through use of the System by IT, or directly by Paciolan, LLC and all compilations thereof, in connection with the operation of the system".

2. Two members of the Events East 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, board members or Events East staff members is owned by Events East and used only to collect feedback for the purposes of HR training and satisfaction surveys. Email addresses used to invite survey participants are safeguarded and only available for Events East use.

[13] Events East was formerly the Trade Centre Limited

Reasons

1. 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 Ticket Atlantic account. In 2004. a tendering process was undertaken to purchase a new ticketing system. Paciolan, LLC. 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, 2020 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, Events East 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) - 71 instances of employee travel outside of Canada with the ability to access personal information through a secure portal into the WCB's internal network via mobile device or remote access.

2. Employee access to personal information by remote access only - 134 individual's personal information (contained in unique claim files) accessed from a remote location outside of Canada (in the US) through a secure portal into the WCB's internal network by remote access.

3. Medical Consultant access to personal information - 37 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.

4. Translation Services - 15 instances of personal information were accessed by translation services procured by Language Line Services. Language Line Services was contracted to provide telephone based language interpreter services for callers whose first language is not English. Language interpreters may be located in any one of a number of countries in or outside North America. Calls involving interpreters are not audio recorded nor do the interpreters document any details of the call; therefore, no recorded information is collected or stored outside of Canada.

5. Disclosure to Contracted Service Provider in a testing situation - An instance of individuals' personal information accessed outside of Canada in the context of upgrading technology to establish an improved operational information storage environment with a contracted service provider. Vendors requiring access to personal information from outside of Canada are granted access on a need to know basis for WCBNS operations, or when expertise does not exist, or is not available in Canada. Agreements and contracts with vendors are in place, and WCBNS IT facilitates this access as needed.

Conditions

1. Employee access to personal information by mobile device (iPhone, iPad, BlackBerry) - Access to WCB's internal network is protected by username/password authentication, and is delivered over a secure portal based on accepted industry practices. Immediate report of theft/loss of device or information.

2. Employee access to personal information by remote access - Access to WCB's internal network is protected by username/password authentication, and is delivered over a secure portal based on accepted industry practices. Immediate report of theft/loss of device or information.

3. Medical Consultant access to personal information - Access to WCB's internal network is protected by username/password authentication, and is delivered over a secure portal based on accepted industry practices. Information limited to only necessary medical information required to complete a review and provide medical report. All consultants have a contract of service that contains strong privacy clauses to protect information.

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

5. Disclosure to Contracted Service Provide in a testing situation - All of the WCB's Privacy Risk 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 information remote access will occur for service reasons/limiting personal information present).

Reasons

1. Employee access to personal information by mobile device (iPhone, iPad, BlackBerry), computer (laptop, desktop) - When staff travel for business or personal purposes and they are expected to monitor their email and voicemail for business continuity, and to fulfill their job-related responsibilities, they must abide by the restrictions noted above.

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

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

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

5. Disclosure to Contracted Service Provide in a testing situation - Current access to and storage of information outside of Canada is tied to WCB programs and/or systems that are necessary for operations. When Privacy Risk Assessments are reviewed for new or upgraded technology special attention is paid to ensure PIIDPA is complied with.

Foreign Access and Storage by Nova Scotia Health Authority and IWK Health Centre

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. In 2017, PIIDPA exceptions were granted for arrangements with the following vendors: Siemens, G.E., Philips Healthcare, Merge Healthcare, Toshiba, Constant Contact, Hill-Rom, and Elekta Ltd.

2. Mobile devise use: For 2017 NSHA reviewed phone records, which indicate 577 instances where mobile devices (e.g. BlackBerry) were used outside of Canada where personal information or company e-mail may have been accessed (Note: report could only retrieve records as far back as Feb 4/17- will remedy for 2018).

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 is required in accordance with PIIDPA. All Privacy Impact Assessments, give consideration to 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. This approval is only for situations where personal information is not involved.

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 2017 calendar year, IWK worked with 92 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 (Obstetrical Trace View, Ecelera System Cardiology)

3. Business Travel - IWK's records indicate that during the 2017 calendar year, there were approximately 94 incidents of travel booked through the IWK* for work-related travel outside of Canada, by 79 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. (*Accounts for travel booked through the IWK's travel provider.)

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 working with service providers where there is potential for storage of, or access to, personal information outside Canada, IWK obtains individuals' consent where practicable, 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 BlackBerrys/iPhones 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 clinical software and medical equipment.

3. Business Travel - The instances of international business travel noted above may not involve the storage or access of personal information outside of Canada. In the event such access/storage does occur, it is for the purposes of facilitating ongoing patient care or research.

Foreign Access and Storage by Universities and Colleges[14]

Acadia University

Description

1. Travel - Acadia staff and faculty participated in international trips in 2017. Employees have access to their email via smart phone, tablet, or laptop. All Acadia employees also have access to Office 365 resources such as email, SharePoint and OneDrive.

2. 0ffice 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. Different components of Office 365 resources are stored in different

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

locations. Exchange (email, calendars, contacts) and Skype for Business are stored in a Canadian datacentre. SharePoint (SharePoint, OneDrive, Groups, Teams) are stored in a North America (U.S.) datacentre.

3. Attend.com - 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. Blackbaud - 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 datacentre is in Vancouver. The vendor provides technical service from time to time via remote access while under the supervision of Divinity personnel.

5. Moodie Learning Management System - Acadia uses Moodie 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. IT 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 datacentre.

7. Enterprise System - Colleague is an Enterprise system that contains employee, alumni, and 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. In addition, Advancement staff, who travel to various international locations, access and enter information regarding donors/alumni while traveling.

8. Email 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. eZRecruit 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.

10. Online elections - electionbuddy.com is an online election software. It is used for student elections and staff groups to determine faculty/staff votes. Those eligible to vote receive a link to a voting website via an email or website portal. It is a cloud-based service with data centres in Canada. It may be accessed, however, when a student or employee is outside of Canada.

11. Turnitin - Turnitin is a software that allows faculty to provide feedback, assess work, and assess plagiarism of student work. It is tied into the Learning Management System (LMS). When a paper is submitted to Turnitin, it is compared against a secure database of licensed source material, including periodicals, academic journals, books, and web pages. Information such as name, email and school are associated with the account. The datacentre currently resides in the United States (California).

12. KnowBe4 - Knowbe4 is a security awareness training system. It provides employees with access to security training sessions, security awareness newsletters and simulated phishing tests and statistics. Information in KnowBe4 is limited to name and email address. The tracking of those who clicked on deliberate unsafe links are recorded against employees' email addresses. The city and country of location of the click is also documented. It will record whether a person is traveling outside of Canada as well. The data is stored in US Amazon datacentres.

13. Orbis - Acadia University Cooperative Education program implemented Outcome provided by Orbis Communications. Outcome is an experiential learning management platform that enables the department to manage their cooperative education program. Data is stored in a Canadian datacentre.

14. Bomgar Remote Support - Used by Technology Services to support users by providing remote access to a user's laptop/desktop. Data is stored at Acadia's data centre. Remote support may be provided to people who are traveling outside of the country.

15. Teamviewer - Used by the Library and Open Acadia to support users by providing remote access to a user's laptop/desktop. Data is stored at Acadia's data centre. Remote support may be provided to people who are traveling outside of the country.

16. Acadia Central - The Acadia student staff portal acts as a central login and launching point for much of the student activity on campus. It has an Acadia datacentre.

Conditions

1. Travel - When accessing outside of Canada, staff are using work related laptops/mobile devices that are password protected as well as authenticated login credentials for access to resources.

2. Office 365 - To access the Office 365 portal, users must have Acadia authenticated credentials and data stored within the Office 365 site is encrypted and secure. To access the Office 365 portal, users must have Acadia authenticated credentials. Data stored within the Office 365 site is encrypted and secure. External access to our SharePoint sites are controlled via authorized access. With the SharePoint architecture, external access is only allowed with certain sites thereby protecting internal departmental sites. Alumni access to O365 resources is through authenticated login. Additional access to SharePoint for particular Alumni (Advancement Life Officers) is through authenticated logins, with further controls set in individual libraries. These alumni are required to sign a privacy/confidentiality agreement with the Office of Advancement.

3. Attend.com - 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. Blackbaud – Alumni/Donor Information. 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. Moodie Learning Management System - 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. IT Ticket Management System - Access to personal information from outside of Canada is limited to authorized personnel, with authenticated logins. It is used to create and monitor service requests.

7. Enterprise System - 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. Off-campus access to Colleague resources is only available through the VPN, with authenticated credentials. Within the firewall, data is protected through login.

8. Email Communication - 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-mydata-onconstant-contact-servers).

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

10. Online elections - electionbuddy.com is a product under the umbrella of RightLabs. Rightlabs provides policies regarding the protection of private and confidential data. The Rightlabs.com Privacy Policy https://rightlabs.com/privacypolicy/.

11. Turnitin - Data is stored in the United States with physical, digital, and procedural safeguards in place to protect personal information, including the use of SSL encryption, redundant servers, and sophisticated firewalls. Passwords are required to access information. At Acadia, authenticated logins are required to access the Learning Management System.

12. KnowBe4 - Access to the system requires an authenticated link to access. Users who have not received an email are not able to login to the system. Once authenticated, users have access to predetermined training sessions. Services run in the cloud, except for a few data sub-processors services and data are hosted in Amazon Web Services (AWS) facilities. The infrastructure, including servers and databases, is spread across multiple AWS data centers for both the US and EU regions and will continue to work should any one of those data centers fail unexpectedly. All the servers are within KnowBe4's own virtual private cloud (VPC} with network access control lists (ACL's) that prevent unauthorized requests getting to our internal network. Customer data is stored in a multi-tenant architecture. There is two-factor authentication (2FA) in place for administrative functions related to the services and for management of the infrastructure.

13. Orbis - Students login into the Acadia Portal via authenticated login. From there, they are redirected to the Orbis portal where an additional authenticated login is required. Students post their job information (resumes etc) against job postings. This can be done from any location. Employers are able to post jobs within the Orbis portal, but they have no access to student

personal information through Orbis. Employers are provided employment packages directly from the Co-Operative office. Acadia staff access Orbis directly (not through the Acadia student portal) using authenticated logins.

14. Bomgar Remote Support - The user must actively provide access to their device. Bomgar Remote Support retains a copy of the contact in logs which are kept for 90 days. The remote support is tied into the university's ticketing system to create a record of the support provided. Bomgar works through the firewall without VPN tunneling, so perimeter security can remain intact. Two factor authentication increases the security of remote access by requiring a second factor (one-time passcode) to login, in addition to the password. Session logging allows for the review of all customer and support representative interactions, and all the events of an individual support session are logged as a text-based log. This log includes representatives involved, permissions granted by the customer, chat transcripts, system information, and any other actions taken by the Bomgar representative.

15. Teamviewer - Access to personal data is controlled by the individual user. The user must actively provide access to their device.

16. Acadia Central - Access to the portal is restricted to authenticated login. Users require an Acadia user ID and password to login. International students require access from their individual home countries. Faculty and staff may access Acadia Central while traveling to fulfil their work functions. Students to access their accounts; faculty and staff to do their work functions.

Reasons

1. Travel - 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. office 365 - Prior to the Office 365 implementation faculty/staff and students were already using cloud-based storage and email on the Acadia network (Google/DropBox). Instead, O365 enables Acadia to have greater security over the file shares.

3. Attend.com - The functionality of Attend.com 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. Blackbaud – The product has been determined to be the best fit for the Divinity College and is widely used in Canada.

5. Moodie Learning Management System - 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. IT Ticket Management System - Team Dynamix is the industry standard for ticketing and project management in the higher education sector.

7. Enterprise System - Employees in Advancement 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. Colleague is provided by Ellucian which along with Banner provides enterprise software to most Canadian universities.

8. Email Communication - Constant Contact is used widely for communication and mass email distribution within the sector.

9. eZRecruit Recruitment - 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.

10. Online elections - electionbuddy is used widely within the education sector.

11. Turnitin - Turnitin is widely used across higher education institutions.

12. KnowBe4 - Ongoing and constant training is a significant step in cyber-security. The cost to create updated and fast-moving training in-house is prohibitive. KnowBe4 provides updated training, newsletters quickly at a reasonable cost.

13. Orbis - Orbis is the industry leader in experiential and career education programs on post-secondary campuses. It was chosen over other products as its datacentre is in Canada.

14. Bomgar Remote Support - Bomgar provides the required product and the ability to support the customer service mandate of Technology Services. Its integration into the ticket and tracking system made it an ideal solution.

15. Teamviewer - Due to costs advantages and timing issues, Open Acadia and Library opted to remain with TeamViewer rather than the Bomgar solution. The product provides reliable service for the library and Open Acadia.

16. Acadia Central - For faculty and staff, access to the system is required to fulfil job requirements. For students, it enables access regardless of their physical location which is necessary for their success at the university.

Cape Breton University

Description

1. Student Information System (theSIS) - 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.

2. 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. Although the system and the data contained in it is maintained on-site, web access is available to this system for both faculty delivering courses and students enrolled in the courses.

3. 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.

4. 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.

5. School/Dude - SchoolDude 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

6. HubSpot - HubSpot is an inbound marketing and sales software platform used by the CBU Marketing and Communications Department. Hubspot has offices in Cambridge Mass; Dublin Ireland; and Sydney Australia. Personal information of CBU contacts and prospective and current systems are held in Hub Spot'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 Hub Spot, and that use of the system is necessary to the operations of the Department.

7. 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 has now opened its Canadian Data Centres, and in the upcoming year all Canadian clients including CBU will be moved to this centre.

8. Office365 - CBU has implemented Office365 for all employees and students. While CBU data in the O365 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.

Conditions

1. Student Information System (theSIS) - Access is only permitted if required as an operational necessity of the university. The system is password protected and access is restricted to need-to-know basis depending on the role of the individual.

2. Course Management System - Access is password protected, and both faculty and students are restricted to the courses they are delivering or are enrolled in.

3. Residence Management - StarRez may require access to the system to resolve technical issues. Access for this reason may be provided for a period of time, under CBU supervision.

4. SharePoint - Access is password protected. Users have access only to sites in which they are registered members.

5. School/Dude - SchoolDude's privacy policy restricts access and distribution of CBU data by the company or its subsidiaries. The department has determined that the system is required for the management of plant maintenance at the university.

6. HubSpot - HubSpot's privacy policy restricts access and distribution of CBU data by the company or its subsidiaries. The department has determined that use of the system is required for the operation of the Marketing and Communication department.

7. Destiny One - Currently, data kept in the system is the minimum required for the delivery of these courses. Access is password protected and restricted to faculty delivering and students enrolled in these non-credit courses.

8. Office365 - Access is password protected and restricted to CBU and students.

Reasons

1. Student Information System (theSIS) - No external storage is permitted. Access is an operational requirement. Employees are trained in the appropriate use of personal information.

2. Course Management System - No external storage is permitted. Access is for course delivery participation only.

3. Residence Management - No external storage is permitted. Access is for technical support only, and is supervised at all times.

4. SharePoint - No external storage is permitted. Access is for university collaboration and is required as considerable travel is undertaken by both faculty and administrators.

5. School/Dude - The university sought a legal opinion on the use of this cloud solution. The opinion was that because personal data stored in this system is available on CBU's public website www.cbu.ca. it was not in violation of the act.

6. HubSpot - The decision was based on operational needs of the department.

7. Destiny One - Access is for course delivery/participation only, and is temporary until the Canadian course is available.

8. Office365 - Storage is within Canada. Access is required for employees and students who may be outside the Country.

Dalhousie University[15]

Description

1. One45 Scheduling and Reporting System - This system is a scheduling, curriculum management, and data reporting solution used by the Faculty of Medicine and the College of Pharmacy. The system will be moving to a cloud based vendor hosted service. Data will be stored in a Canadian cloud, but technical support and access can occur outside of Canada.

2. MoveON Software - This integrated software is used to manage international partnership agreements and student and faculty mobility activities. Data is stored in a Canadian data

[15] Report includes the Nova Scotia Agricultural College

center, but a secondary backup is stored in France. Access for the purpose of technical support can occur outside of Canada.

3. Undergraduate Medical Education Exam System - See description of storage and access provided in the 2016 annual PIIDPA report.

4. Community Health & Epidemiology (CH&E) Process Improvement - See description of storage provided in the 2016 annual PIIDPA report.

5. Continuing Education Software - See description of storage provided in the 2016 annual PIIDPA report.

6. Lecture Capture & Streaming Media Solution - See description of storage provided in the 2016 annual PIIDPA report.

7. ACHA-NCHA National College Health Assessment Student Survey - See description of storage provided in the 2016 annual PIIDPA report.

8. Plagiarism Detection Software - See description of storage provided in the 2016 annual PIIDPA report.

9. Educational Technology Apps - See description of storage provided in the 2016 annual PIIDPA report.

10. Insights, Pulse, Wiggio and Video Note - See description of storage provided in the 2016 annual PIIDPA report.

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

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

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

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

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

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

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

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

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

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

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

22. Teaching and Research Statistical 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. Plagiarism Detection - See description of storage provided in the 2012 annual PIIDPA report.

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

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

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

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

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

Conditions

1. One45 Scheduling and Reporting System - The vendor has in place written privacy and security policies and procedures to protect the privacy of personal information and periodic monitoring of the vendor and subcontractor's security measures will be undertaken by the Faculty of Medicine's IT department. The vendor has implemented strong user access controls to ensure only the necessary staff are able to access data for support purposes. The methods for access are secure. Contractual obligations and a non-disclosure agreement protect the confidentiality of information.

2. MoveON Software - The number of system administrators outside of Canada who can access data for support purposes is extremely limited. Strong user access controls are in place and the methods for access are secure. The secondary backup is encrypted in Canada before it is transferred to France. The data is only decrypted in Canada. The vendor is ISO 27001 certified and contractual obligations are in place to protect the privacy and security of information.

3. Undergraduate Medical Education Exam System - See description of storage and access provided in the 2016 annual PIIDPA report.

4. Community Health & Epidemiology (CH&E) Process Improvement - See description of storage provided in the 2016 annual PIIDPA report.

5. Continuing Education Software - See description of storage provided in the 2016 annual PIIDPA report.

6. Lecture Capture & Streaming Media Solution - See description of storage provided in the 2016 annual PIIDPA report.

7. ACHA-NCHA National College Health Assessment Student Survey - See description of storage provided in the 2016 annual PIIDPA report.

8. Plagiarism Detection Software - See description of storage provided in the 2016 annual PIIDPA report.

9. Educational Technology Apps - See description of storage provided in the 2016 annual PIIDPA report.

10. Insights, Pulse, Wiggio and Video Note - See description of storage provided in the 2016 annual PIIDPA report.

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

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

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

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

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

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

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

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

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

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

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

22. Teaching and Research Statistical 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. Plagiarism Detection - See description of storage provided in the 2012 annual PIIDPA report.

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

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

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

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

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

Reasons

1. One45 Scheduling and Reporting System - The system's move to a cloud based vendor hosted service is needed to:
    - Enable the use of the only reporting solution that meets the requirements of the Royal College of Physicians and Surgeons' Competence by Design Initiative; and
    - Meet One45's operating system requirements.

2. MoveON Software - The MoveON software is needed to support the effective and efficient management of Dalhousie's international programs. Its use allows the University to:
    - simplify the management of international partnership relationships, agreements, and student/faculty/staff mobility programs; and
    - improve coordination among academic and administrative units directly involved with international activities.

3. Undergraduate Medical Education Exam System - See description of storage and access provided in the 2016 annual PIIDPA report.

4. Community Health & Epidemiology (CH&E) Process Improvement - See description of storage provided in the 2016 annual PIIDPA report.

5. Continuing Education Software - See description of storage provided in the 2016 annual PIIDPA report.

6. Lecture Capture & Streaming Media Solution - See description of storage provided in the 2016 annual PIIDPA report.

7. ACHA-NCHA National College Health Assessment Student Survey - See description of storage provided in the 2016 annual PIIDPA report.

8. Plagiarism Detection Software - See description of storage provided in the 2016 annual PIIDPA report.

9. Educational Technology Apps - See description of storage provided in the 2016 annual PIIDPA report.

10. Insights, Pulse, Wiggio and Video Note - See description of storage provided in the 2016 annual PIIDPA report.

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

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

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

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

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

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

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

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

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

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

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

22. Teaching and Research Statistical 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. Plagiarism Detection - See description of storage provided in the 2012 annual PIIDPA report.

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

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

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

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

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

Mount Saint Vincent University

Description

1. 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. The information they have access to is maintained on a server controlled by Mount Saint Vincent University (within Canada).

2. NSSESurvey - During 2017, 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 the prohibition of any subsequent use or disclosure of that information in individually identifiable form without the express authorization of MSVU.

3. Offlce365 - Mount Saint Vincent University students, faculty and staff have access to Microsoft's Office 365 suite of online applications and services, including email, calendar, OneDrive cloud storage, SharePoint Online, and numerous other Office 365 applications. Data at rest for most of Office 365 services, including email, calendar, OneDrive, and SharePoint, reside In Microsoft's Canadian datacenters, but some Office 365 services store data outside Canada. The University documents which Office 365 services store data outside Canada on the University website. Office 365 services are used for teaching, administration, and personal use.

Conditions

1. 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.

2. NSSESurvey - The research agreement with the Indiana University for the Mount's participation in the NSSESurvey 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.

3. Offlce365 - Office 365 services are protected by industry standard security measures, including password authentication, firewalls, intrusion detection systems, encryption of at-rest and in-transit data, and anti-malware and anti-spam software. Office 365 authentication occurs through University owned and controlled servers. Microsoft datacenters are physically secured to prevent unauthorized access.

Reasons

1. General - 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.

2. NSSESurvey - 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.

3. Offlce365 - Office 365 is a standard service offering for Nova Scotian universities, and was implemented under a program of the Higher Education Information Technology Shared Services (HISS) organization. The security protections offered by Office 365 are higher than could otherwise be accomplished, and Office 365 offers functionality that is necessary to maintain competitive educational technologies.

Nova Scotia College of Art and Design

Description

1. We use Microsoft Office 365 for email, collaboration and personal storage. This product is now the standard for Universities in the Province of Nova Scotia. As a group, the Universities in Nova Scotia continue to work with Microsoft to have all functional storage maintained at data centers in Canada. However, access to this software can occur from anywhere in the world.

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 remotely in case 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 access is controlled by robust authentication and security group protection. The University provides training on security and privacy and further provides alternative file services and methodologies that allow users to keep select information 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. Password management is kept to best practices.

3. Access to information is 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 only via access to a virtual private network.

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 has helped promote best practices in data management and storage.

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 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.

Nova Scotia Community College

Description

1. As required by section 5(3) of the Personal Information International Disclosure Protection Act (PIIDPA) the Nova Scotia Community College (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. In 2016, NSCC completed its migration of electronic mail to Microsoft Office 365 in collaboration with the Higher Education Information Technology Shared Services organization. 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. This migration was completed in late 2017.

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.

4. NSCC uses software-as-a-service applications in support of teaching, learning and professional development. Brightspace, Safe Colleges and Lynda.com store limited personally identifiable information regarding students and staff on servers located outside of Canada. In the case of Brightspace, a migration to Canadian data centres is planned for 2018.

5. 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 promoting Microsoft's OneDrive for Business offering as an alternative as this will keep data in Canada.

Conditions

See above.

Reasons

See above.

St. Francis Xavier

Description

1. One Solution: See description of access and /or storage provided in the 2016 annual PIIDPA report.

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

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

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

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

6. 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. Qualtrics: See description of access and /or storage provided in the 2016 annual PIIDPA report.

9. Fluid Review: See description of access and /or storage provided in the 2016 annual PIIDPA report.

10. Employees Travelling Email: See description of access and /or storage provided in the 2016 annual PIIDPA report.

11. Interview stream is used by the student career center to assists students in developing interview skills. Interview stream is based in Chicago IL and data is stored in the United States.

12. University Tickets is a program used to generate tickets and verify student IDs for athletic events on campus. University Tickets is based out of New York, NY and data is stored in the US.

13. Office 365 is available to staff, faculty and students, 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. StFX is a Canadian tenant of the package with most services stored in Canada but there are programs that are stored in the US.

14. Team Dynamix is used by the Information Technology department for Information Technology Service Management. TDX is based out of Columbus OH and data is stored in the US on Microsoft Azure infrastructure.

Conditions

1. See reasons for access and or storage provided in the 2016 annual PIIDPA report.

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. See reasons for access and or storage provided in the 2016 annual PIIDPA report.

9. See reasons for access and or storage provided in the 2016 annual PIIDPA report.

10. See reasons for access and or storage provided in the 2016 annual PIIDPA report.

11. Access to information outside of Canada is limited to vendor support that is requested by the University or limited to StFX users who may be out of the country but need access to information. Information is protected and limited to authorized users through industry standard data security, encryption and authentication practices.

12. Access to information outside of Canada is limited to vendor support that is requested by the University or limited to StFX users who may be out of the country but need access to information. Information is protected and limited to authorized users through industry standard data security, encryption and authentication practices.

13. Access to information outside of Canada is limited to vendor support that is requested by the University or limited to StFX users who may be out of the country but need access to information. Information is protected and limited to authorized users through industry standard data security, encryption and authentication practices.

14. Access to information outside of Canada is limited to vendor support that is requested by the University, Microsoft Azure infrastructure authorized personnel, or limited to StFX users who may be out of the country but need access to information. Information is protected and limited to authorized users through industry standard data security, encryption and authentication practices.

Reasons

1. See reasons for access and or storage provided in the 2016 annual PIIDPA report.
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. See reasons for access and or storage provided in the 2016 annual PIIDPA report.
9. See reasons for access and or storage provided in the 2016 annual PIIDPA report.
10. See reasons for access and or storage provided in the 2016 annual PIIDPA report.
11. The Vendor was chosen for best meeting operational needs, functionality, data security and cost as compared to known alternatives.
12. The Vendor was chosen for best meeting operational needs, functionality, data security and cost as compared to known alternatives.
13. The Vendor was chosen for best meeting operational needs, functionality, data security and cost as compared to known alternatives.
14. The Vendor was chosen for best meeting operational needs, functionality, data security and cost as compared to known alternatives.

St. Mary's University

Description

1. Plagiarism Detection: See description of access or storage provided in the 2012 annual PIIDPA report.
2. Travel: See description of access or storage provided in the 2012 annual PIIDPA report.
3. Qualtrics: See description of access or storage provided in the 2014 annual PIIDPA report.
4. Saint Mary's University Commercial Card Program: See description of access or storage provided in the 2014 annual PIIDPA report.
5. Evernote: See description of access or storage provided in the 2015 annual PIIDPA report.

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

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

8. Mailchimp: See description of access or storage provided in the 2016 annual PIIDPA report.

9. StarRez: See description of access or storage provided in the 2016 annual PIIDPA report.

10. Trello: Trello is a web-based team collaboration tool that organizes projects into visual boards with cards. It is used when working on projects, programs, workshops etc.

11. Typeform: Typeform is used to collect RSVPs and evaluations for campus events.

Conditions

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

2. See restrictions or conditions 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 PIIDPA report.

5. See restrictions or conditions provided in the 2015 annual PIIDPA report.

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

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

8. See restrictions or conditions provided in the 2016 annual PIIDPA report.

9. See restrictions or conditions provided in the 2016 annual PIIDPA report.

10. Personal information such as name and email addresses may be stored on US servers.

11. Personal information such as name and address is collected when the form is completed.

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 2015 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 2016 annual PIIDPA report.

9. See details provided in the 2016 annual PIIDPA report.

10. While there are a number of collaboration tools on the market, none are hosted on Canadian servers, at this time.

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

Université Sainte-Anne

Description

1. Blackbaud: Student information system that contains personal information and our students' academic record. Personnel and students may access Blackbaud while on travel or at home (international students). The Université has been using Blackbaud for several years.

2. Moodle: Students and professors can access our course management system in order to offer and follow our course offerings. Access is protected via the use of passwords, but can be accessed from anywhere around the world. The information is however stored in Canada.

3. Office 365: Personnel and students of the Université have access to Office 365 which provides access resources such as e-mails, SharePoint and OneDrive.

Conditions

1. The Université has a signed agreement with the provider that no one in the US is to access the personal information, unless required by law. For our own users, passwords are required to access the database.

2. Only personnel with a valid password can access the course management system.

3. Access to the Office 365 portal is password protected.

Reasons

1. Required to assure daily operations of the Université.

2. Access to our course management system is necessary by our personnel and students in order to assure the daily operations of the Université.

3. Access to the Office 365 portal is essential to maintain the daily operations of the Université.

University of King's College

Description

1. Only additions to our 2017 PIIDPA report: No additions for calendar year 2017.

Conditions

1. Only additions to our 2017 PIIDPA report: No additions for calendar year 2017.

Reasons

1. Only additions to our 2017 PIIDPA report: No additions for calendar year 2017.

Foreign Access and Storage by School Boards

Annapolis Valley Regional School Board

Description

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

2. Use of Social Media – Twitter – AVRSB and a number of its schools operate a Twitter account. Twitter is based in the United States. This account is used for sharing news releases, videos, photos and other information to a broader audience.

3. Khan Academy - Khan Academy resources and interactive lessons are available on a variety of subjects, including mathematics, computer programming, science, finance, history, and the humanities. Additional apps and resources may be identified as having educational value and may be downloaded or accessed to the devices provided. Personal information about students and teachers will be accessed and stored outside Canada as the Khan Academy is located outside Canada.

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

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

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

administration to administer the program.

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

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

3. 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 fictitious or a combination of three initials and five to six numbers, to reduce the ability to easily identify an individual, their gender, or ethnicity.

4. 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 System - The Department of Education and Early Childhood Development and AVRSB have signed a contract extension through June of 2018 with Frontline Technology that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by the Department of Education and Early Childhood Development and the School Board in writing. Frontline has read and agreed to the provisions of PIIDPA. The contract also has extensive provisions for protection of personal information, including the requirement for Frontline to notify the Department of Education and Early Childhood Development 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 Development monthly. Access is only for the period of time required to address the issue/problem, and access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. Frontline's SunGard data facility is audited regularly by independent firms to ensure verification of process and discipline. The facility is OSO 9001:2000 certified by Lloyd's Registry Quality Assurance. Employees of Frontline have signed confidentiality agreements with the company. Only

personnel authorized by AVRSB are provided access to the School Board's electronic information. The data contained in the system is limited to that required to ensure successful operation.

6. International Baccalaureate Diploma Program - Parents/guardians receive information about the IB program, including that it is administered outside Canada through offices in Switzerland and the United Kingdom.

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

Reasons

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

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

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

5. Aesop System - 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. The AP program is administered by The College Board, a

not-for-profit organization in New York. AP courses give students access to rigorous college-level work. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

Atlantic Provinces Special Education Authority

Description

1. A number of staff travelled outside Canada for business and/or pleasure, and had the ability to access personal information using cell phones.

Conditions

1. Staff are required to have permission prior to taking devices out of Canada. Devices are password protected.

Reasons

1. N/A

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, photos and other information to a broader audience.

2. The Cape Breton-Victoria Regional School Board utilizes the Aesop system provided by Frontline Technologies Canada (FTC), which is an automated tool used for tracking, processing and storing information related to employees' absences. The software and data reside in Toronto, Ontario. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. The system is supported and maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA.

3. Khan Academy was partnered with Hour of Code and Code.org which was also endorsed by the DEECD. Khan Academy resources and interactive lessons are available on a variety of subjects, including mathematics, computer programming, science, finance, history, and the humanities. Additional apps and resources may be identified as having educational value and may be downloaded or accessed to the devices provided. Personal information about students and teachers will be accessed and stored outside Canada as the Khan Academy is located outside Canada.

4. 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.

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

6. 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.

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 birthdates 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. 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.

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

6. 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.

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. 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.

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

6. 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.

Chignecto-Central Regional School Board

Description

1. Travel with Electronic Devices - See description of access and/or storage provided in the 2016 PIIDPA Report.

2. Use of Social Media - See description of access and/or storage provided in the 2016 PIIDPA Report.

3. AESOP - See description of access and/or storage provided in the 2016 PIIDPA Report.

Conditions

1. Travel with Electronic Devices - Same as above

2. Use of Social Media - Same as above

3. AESOP - Same as above

Reasons

1. Travel with Electronic Devices - Same as above

2. Use of Social Media - Same as above

3. AESOP - Same as above

Conseil Scolaire Acadien Provincial

Description

1. Travel Outside Canada - A number of CSAP staff members travelled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in the Microsoft Outlook email system, using devices including cell phones, iPads, BlackBerrys and laptops.

2. Google Apps for Education - The CSAP's students, teachers and administrators use 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 as domain exclusive websites that can be shared with both internal and external users.

3. Use of Social Media
    a. Twitter: The CSAP and several schools operate a Twitter account. Twitter is based in the United States. This account is used for sharing government news releases, videos, photos and other information to a broader audience.
    b. Facebook: The CSAP 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.

4. 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.

5. International Baccalaureate Diploma Program - The CSAP 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.

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

7. Powtoon - Some CSAP schools use Powtoon to create educational presentations and videos.

8. Netmaths - Netmaths is an online learning platform, individualized by students where they can practice Math skills from Primary to Grade 12 and receive reports on their progress. Skills are aligned to the Nova Scotia Curriculum.

9. Esri Canada Arcgis Online - Teachers uses ArcGIS Online to create and share interactive maps. Ready-to-use maps are available, as well as the technology to create new maps which use data and tell a story. Esri's Education branch offers several entry level software which enables students and teachers to engage in big data and cross-curricular understanding.

10. ClassDojo - ClassDojo allows teachers to publish the work of their students in a moderated environment and allows for feedback from the parents. Basic enrolment is free.

11. Screencast - Screencast is used by CSAP teachers to download a variety of audio-visual feedbacks and by students to view these feedbacks.

12. Prezi - Prezi is used by CSAP teachers to create non-linear educational presentations. The platform allows the teacher to present and exploit dynamic learning situations that can motivate and engage students. Students can also use Prezi to create dynamic presentations.

Conditions

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

2. Risk mitigation strategies are in place to reduce risks to personal information, including users informing 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.

3. Use of Social Media:
    a. Twitter: The CSAP uses Twitter to share information and interact online with the public and organizations in social spaces. The CSAP collects no IP addresses or personal information through these services. The CSAP retweets other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.)
    b. Facebook: The CSAP posts information related to the wider school community and may share other government posts, announcements and/or public safety information from partners. As with Twitter, the Board collects no IP addresses or personal information through these services. Photos and videos that are posted to all social media platforms have written consent from the people in them where required.

4. It is recommended that teachers set up Khan Academy student accounts so that students, 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 dates entered for all students and teachers were fictitious, and the field indicating gender was left blank. It was recommended that usernames be the student's or teacher's three initials plus 5-6 numbers, to reduce the ability to easily identify an individual, their gender, or ethnicity.

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

6. Teacher's name and school name are required for the subscription.

7. Teacher's name and email are required for the subscription. Teachers are not required to reveal any other personal information as a result of creating the free account. Students will never be required to reveal personal information.

8. It is recommended that the minimum personal information is provided about students and teachers at the point of setting up new accounts.

9. Teacher registers using full name, school and email address. Once they are registered they register their students under their account. Teacher can use aliases to sign up students. The

ESRI respects the right to privacy and will not collect any personal information on this website without permission.

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

11. Teacher's name, email and country are required for the subscription. Teachers are not obliged to give additional information after the creation of the free account and the students give no personal information.

12. Teacher's name and email are required for the subscription. Teachers are not obliged to give additional information after the creation of the free account. Students can log in with their Google accounts.

Reasons

1. Staff are expected to monitor their email and voicemail for business continuity purposes, and maintain contact with operations. Cellular phones were necessary to access email and Internet sites, and make telephone calls. Laptops etc. are needed for preparing documents, and accessing email and Internet sites. Staff members accompanying students are required to have in their possession or the ability to rapidly access personal information in case of emergencies while away.

2. 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 staff, teachers and students to access these resources both within and outside the school, and provides a measure of equity for all.

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

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

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

6. There is no Canadian alternatives identified.

7. Powtoon is the only free cloud software that can create videos of this type that are easily accessible.

8. Netmaths is designed by an educational technology laboratory in Quebec to meet the mathematical needs of the French-speaking population in Canada and elsewhere. There is no acceptable equivalent located within Canada.

9. Highest standards of security and confidentiality, strictly in accordance with the Data Protection Acts, 1988 & 2003. No alternative exists in Canada.

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

11. Screencast is one of the only ways to easily and quickly provide descriptive feedback to students in a free and cryptic environment. Students only watch videos and are kept out of the cloud system.

12. Prezi encourages students to get involved in the classroom with interactive charts and infographics. It is one of the most important reporting and analysis tools. It has valuable visualization features that are unlike any other program.

Halifax Regional School Board

Description

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

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

3. Khan Academy - Khan Academy resources and interactive lessons are available on a variety of subjects, including mathematics, computer programming, science, finance, history, and the humanities. Additional apps and resources may be identified as having educational value and may be downloaded or accessed to the devices provided. Personal information about students and teachers will be accessed and stored outside Canada as the Khan Academy is located outside Canada.

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

5. Aesop - The Halifax Regional School Board utilizes the Aesop System provided by Frontline Technologies Canada (FTC), which is an automated tool used for tracking, processing and storing information related to employees' absences. The software and data reside in Toronto, Ontario. The system is accessed remotely by schools and the School Board using the internet and telephone Interactive Voice Response (IVR) system. The system is supported and

maintained by FTC's parent company Frontline Placement Technologies (FPT) located in Philadelphia, USA. Frontline Placement Technologies require periodic access to the data in order to respond to requests received from the School Board and to perform system maintenance and support.

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

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

Conditions

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

3. Khan Academy - Khan Academy resources and interactive lessons are available on a variety of subjects, including mathematics, computer programming, science, finance, history, and the humanities. Additional apps and resources may be identified as having educational value and may be downloaded or accessed to the devices provided. Personal information about students and teachers will be accessed and stored outside Canada as the Khan Academy is located outside Canada.

4. Google Apps for Education - 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 Halifax Regional School Board have signed a further five-year contract with Frontline Technology that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by the Department of Education and Early Childhood Development 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 Development 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 Development monthly. Access is only for the period of time required to address the issue/problem, and access is only carried out from within Canada or from the supplier's secure private network in Philadelphia. Aesop's storage facility is audited regularly by independent firms to ensure verification of process and discipline. The facility is OSO 9001:2000 certified by Lloyd's Registry Quality Assurance. Employees of Frontline have signed confidentiality agreements with the company. Only personnel authorized by the Halifax Regional School Board are provided access to the School Board's electronic information. The data contained in the system is limited to that required to ensure successful operation.

6. 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 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.

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

5. 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. The AP program is administered by The College Board, a not-for-profit organization in New York. AP courses give students access to rigorous college-level work. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

South Shore Regional School Board

Description

1. 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. 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 South Shore Regional School Board operates a Twitter account. Twitter is based in the United States. This account is used for sharing government news releases, videos, photos and other information to a broader audience. b) Facebook: 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. Showbie - Showbie allows teachers with one-to-one classroom environments to set up a paperless learning management system that is Universal Design for Learning friendly. Selected teachers (with Showbie PRO licenses) and their selected students may set up classes to distribute and receive work from some or all of their students. It is also an exceptionally seamless option for classroom teachers/ resource teachers and learning centre teachers to deliver accessible digital content to access and engage in the curriculum (not necessarily in a one-one environment.)

5. 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.

6. 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.

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

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

Conditions

1. 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) Twitter: The South Shore Regional School Board uses Twitter to share information and interact online with the public and organizations in social spaces. The South Shore Regional School Board collects no IP addresses or personal information through these services. The South Shore Regional School Board retweets other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.) b) Facebook: 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 of personal information is provided about students and teachers at the point of setting up new accounts. For example, it was recommended that the birth dates entered for all students and teachers were fictitious, and the field indicating gender was left blank. It was recommended that usernames be the student's or teacher's three initials plus 5-6 numbers, to reduce the ability to easily identify an individual, their gender, or ethnicity.

4. Showbie - Users are not required to input any personal information - it is optional but not required. There is a privacy policy and a terms of use agreement. Staff are also required to inform parents/guardians that particular teachers will be using the service in conjunction with their student. No additional personal information is requested.

5. 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.

6. Aesop - The Department of Education and Early Childhood Development and The South Shore Regional School Board have signed a further five year contract with Frontline Technology that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by the Department of Education and Early Childhood Development 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 Development 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 Development 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 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.

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

8. 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 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. Showbie - The Teacher PRO version of Showbie allows for seamless integration with other cross-curricular creation apps such as Google Docs, Book Creator, iMovie, Pages, Keynote, Explain Everything, etc. Teachers can present information for students so that it is accessible

by all (including audio and video formats) and they can leave instructions and feedback for students in multiple formats. Showbie enhances student engagement and helps hold them accountable for their learning. It is easily shared with parents/guardians. We do not believe there is another option which is as user-friendly for all involved and is as accessible for all students (from a Universal Design for Learning approach).

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

6. 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."

7. 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.

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

Strait Regional School Board

Description

1. Travel with electronic devices - A number of Strait Regional School Board staff traveled outside Canada for business and/or pleasure, and had the ability to access personal information contained in email or stored in the Zimbra 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 Strait Regional School Board operates a Twitter account. Twitter is based in the United States. This account is used for sharing government news releases, videos, photos and other information to a broader audience. b) Facebook: The Strait 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. Google Apps for Education - The Strait Regional School Board's students, teachers and administrators use Google Apps for Education, including services such as Drive, Sites, Gmail, Calendar, Groups and Contacts. Users may create, store online, and share documents,

presentations, spreadsheets, etc. as well as domain exclusive web sites that can be shared with both internal and external users. The service can also provide a complete email, calendar and contacts function that can be configured for an educational domain of choice.

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

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

6. 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.

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

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

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

10. ClassDojo - ClassDojo is a classroom communication app used to share reports between parents and teachers. Teachers track student behavior, post student work, bulletin boards and school notices. The gamification style system teaches developmental skills through real-time feedback.

11. Reflex Math - Reflex Math is an online learning platform that helps students solidify basic math skills. It's an app that can be used on a computer or tablet.

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) Twitter: The Strait Regional School Board uses Twitter to share information and interact online with the public and organizations in social spaces. The Strait Regional School Board collects no IP addresses or personal information through these services. The Strait Regional School Board retweets other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.) b) Facebook: The schools 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. 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.

4. Aesop - The Department of Education and Early Childhood Development and The Strait Regional School Board have signed a further five-year contract with Frontline Technology that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by the Department of Education and Early Childhood Development 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 Development 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 Development 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 Strait Regional School Board are provided access to the School Board's electronic information. The data contained in the system is limited to that required to ensure successful operation.

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

6. 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 dates entered for all students and teachers were fictitious, and the field indicating gender was left blank. It was recommended that usernames be the student's or teacher's three initials plus 5-6 numbers, to reduce the ability to easily identify an individual, their gender, or ethnicity.

7. Raz Kids - Personal information of students is not shared. An identifier is provided by the teacher (i.e. number or initials).

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

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

10. ClassDojo - Students' full names are not used; only first names or initials. Some non-identifying (back of head) student photos were posted. A few parents sent pictures to the teacher through the class Dojo messaging system. Written parental permission is sought for all students. At the end of the school year the teacher archives/deletes the information.

11. Reflex Math - There is no identifying information. Each student in the class is assigned a number from 1 – 15 and the students log in as Student1, Student2, etc. Personal information is not shared. There is no identifying information on students or their grade level.

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

4. 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."

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. 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.

7. Raz Kids – n/a

8. Mathletics – n/a

9. IXL – n/a

10. ClassDojo – n/a.

11. Reflex Math – n/a

Tri-County District School Board[16]

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 Zimbra 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 Regional School Board operates a Twitter account. Twitter is based in the United States. This account is used for sharing government news releases, videos, photos and other information to a broader audience. b) Facebook: The Tri-County 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 Tri-County 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 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

[16] The Council on African Canadian Education did not submit a PIIDPA Form 1.

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 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.

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

Conditions

1. 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) Twitter: The Tri-County Regional School Board uses Twitter to share information and interact online with the public and organizations in social spaces. The Tri-County Regional School Board collects no IP addresses or personal information through these services. The Tri-County Regional School Board retweets other government accounts and public safety information from partners (RCMP, municipality, school boards, etc.) b) Facebook: 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 of personal information is provided about students and teachers at the point of setting up new accounts. For example, it was recommended that the birth dates entered for all students and teachers were fictitious, and the field indicating gender was left blank. It was recommended that usernames be the student's or teacher's three initials plus 5-6 numbers, to reduce the ability to easily identify an individual, their gender, or ethnicity.

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 Tri-County Regional School Board have signed a further five-year contract with Frontline Technology that clearly states the information will be kept private and confidential and will not be released to any third party unless authorized by the Department of Education and Early Childhood

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

5. 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. The AP program is administered by The College Board, a not-for-profit organization in New York. AP courses give students access to rigorous college-level work. The program provides an internationally accepted qualification for entry into higher education, and is accepted by many universities worldwide. There is no Canadian equivalent.

Foreign Access and Storage by Municipalities[17]

Cape Breton Regional Municipality [18]

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. We do require each employee traveling outside the country with a CBRM Device (laptop. smart phone. Tablet) to register the dates and country of travel to the Department of Technology. All data storage is within Canada therefore there is no restriction necessary on data storage.

---

[17] Municipality of the County of Cumberland, Municipality of the County of Richmond, 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 Annapolis Royal (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, Municipal Effectiveness Advisory Committee, Board of Police Commissioners, Investment Committee), 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, 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.

[18] Report includes Cape Breton Regional Police Service.

Reasons

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

Halifax Regional Municipality[19]

Description

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

2. 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.

3. 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

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

9. 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.

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

11. 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.

12. DELL (Storage Area Network, VMWare, SecurID) with a headquarters in North York, ON were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

13. 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.

14. Accenture, with several regional offices in Canada, including Fredericton, New Brunswick were provided access on an approved, need basis to the ServiceNow development and production environments for support and enhancement purposes.

15. 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.

16. 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.

17. 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.

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

19. Micro Focus (Backup Software) 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.

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

21. MailChimp (Email Subscription Services) with a headquarters in Georgia, US.

22. Survey Monkey, with a Canadian headquarters in Ottawa, ON, HRM's data is hosted in Canada.

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

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

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

26. Desire2Learn (D2L) - Brightspace, Learning Management System, with a headquarters in Kitchener, ON.

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

28. 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.

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

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

31. Legend Recreation Software, with a headquarters in Ottawa, ON, HRM's data is hosted in Canada.

32. Pictometry Connect & Pictometry Image Service with a headquarters in Bothell, WA is used as an enhancement to the municipality's Geographical Information System (GIS).

33. FDM (Aptean) with a Canadian headquarters in Vancouver, BC were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

34. Lenel, United Technologies (Security Solutions) of Farmington, CT were provided access on an approved, need basis to the applicable production systems for support and maintenance purposes.

35. Between January 1st and December 31st, 2017, thirty-seven (37) staff travelled outside of Canada to the United States, five (5) staff travelled outside of Canada to Europe and two (2) staff travelled outside of Canada to the Caribbean, one (1) staff travelled outside of Canada to South America, one (1) staff travelled outside of Canada to Central America and had the ability to access personal information via one or more of the following means: Cell Phone, BlackBerry, Laptop, Memory Stick, VPN.

36. CIBC, with a Canadian headquarters in Toronto, ON provide banking and/or investment services.

37. RBC Bank, RBC Investor Services and RBC Dominion Securities, with a Canadian headquarters in Toronto, ON provide banking and/or investment services.

38. TO Bank and TO Securities, with a Canadian headquarters in Toronto, ON provide banking and/or investment services.

39. BMO, with a Canadian headquarters in Montreal, QC provide banking and/or investment services.

40. National Bank Financial, with a Canadian headquarters in Toronto, ON provide banking and/or investment services.

Conditions

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

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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

21. Registration by the Volunteers for the notification service is voluntary and consent is obtained at time of sign-up.

22. Registration for the service is voluntary and consent is obtained at time of sign-up.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Reasons

1. Vendor access is necessary for the system to continue to function properly.
2. Vendor access is necessary for the system to continue to function properly.
3. Vendor access is necessary for the system to continue to function properly.
4. Vendor access is necessary for the system to continue to function properly.
5. Vendor access is necessary for the system to continue to function properly.
6. Vendor access is necessary for the system to continue to function properly.
7. Vendor access is necessary for the system to continue to function properly.
8. Vendor access is necessary for the system to continue to function properly.
9. Vendor access is necessary for the system to continue to function properly.
10. Vendor access is necessary for the system to continue to function properly.
11. Vendor access is necessary for the system to continue to function properly.
12. Vendor access is necessary for the system to continue to function properly.
13. Vendor access is necessary for the system to continue to function properly.
14. Vendor access is necessary for the system to continue to function properly.
15. Vendor access is necessary for the system to continue to function properly.
16. Vendor access is necessary for the system to continue to function properly.
17. Vendor access is necessary for the system to continue to function properly.
18. Vendor access is necessary for the system to continue to function properly.
19. Vendor access is necessary for the system to continue to function properly.
20. 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.
21. MailChimp is highly ranked as one of the best products and seamlessly integrates with the municipality's content management system, Drupal. A 2017 market comparison of the top 10 products confirmed they were all hosted outside of Canada.

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

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

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

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

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

27. 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.

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

29. 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.

30. 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.

31. 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.

32. The municipality partners with PVSC who use the Pictometry vendor and this provides the best financial value for the municipality.

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

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

35. The 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.

36. 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.

37. 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.

38. 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.

39. 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.

40. 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, 2017 forty-eight (48) Halifax Water staff were permitted to transport personal information devices such as laptop computers, cell phones, and electronic data storage devices outside Canada seventy-eight (78) times.

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

Conditions

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

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

Reasons

1. Halifax Water 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[20]

Description

1. 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.

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

Conditions

1. 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 include:
    - Requiring them to report any breaches of security or unusual access (including the *Patriot Act*)

   Reaffirming the exact purpose for which the information is provided and that only the County can provide permission for it to be accessed for other purposes.

Reasons

1. In 2014, other municipal units were surveyed in Nova Scotia (as well as a few in New Brunswick) to gather names of providers used for payroll services. The highest percentage of respondents indicated they were using ADP as their payroll service provider. Other service providers were invited to demonstrate their software. However, it was determined that ADP was the better solution with the ability to grow and expand with our needs. Additionally, this product allowed historical data to be "rolled into" the new product alleviating the need for dependence on paper copies. An options memorandum and Privacy Impact Assessment were prepared and submitted to the Chief Administrative Officer.

Municipality of the County of Antigonish

Description

1. Ironflow Technologies Inc. - Staff vacation and leave time tracking application- used since Nov 2016. Information shared through this program: staff names, positions and departments, vacation and leave scheduling, email addresses. Data storage information from their website: *Is Timeoffmanager secure and confidential? Where is the data hosted, and is it safe? Your information is kept safe and secure, at all times! All our servers are hosted and professionally managed by Contegix. We also use HTTPS to transfer data from your computer to our servers, so all communications are encrypted to ensure privacy.* Contegix: American company with data centres in MO, PA, TX, and Amsterdam.

2. PathFive (Rec Software) - Online recreation department registration program that facilitates online registration for Recreation programs. From terms and conditions: *3.1.3 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. 3.1.4. Dreamstalk will only Handle User Data in its possession to the extent required to provide the Service and shall perform its obligations under the Agreement in compliance with all applicable Canadian privacy laws. Without limiting the generality of the foregoing:*

a) Dreamstalk shall take all reasonable measures to ensure that User Data in its custody or control is protected against theft, loss and unauthorized use or disclosure.

b) Whenever Dreamstalk transfers User Data over the internet, it will employ appropriate cryptographic protocols such as Secure Sockets Layer (SSL) encryption.

c) Dreamstalk shall keep confidential all User Data and will not disclose User Data to third parties (which for clarity does not include Stripe Connect, its employees and agents, to the extent such persons require such User Data for the purpose of Dreamstalk's provision of the Service), except as may be required by law.

d) *Dreamstalk will notify the Customer immediately upon becoming aware that any User Data has been stolen, lost, or accessed by unauthorized persons.*
e) *This company was bought out by the software company Aptean.*

Conditions

1. Limited information about users are inputted into this program; only what is necessary (name, email, start date, leave dates) for function; "optional" information (phone numbers, salary, addresses) not given.

2. Stripe Connect is the payment component of the software. No restrictions of storage or access have been placed on its use as part of the Path Five program.

Reasons

1. Significant operational time savings were realized by using this software.

2. Stripe Connect is an embedded component required to use software from a Canadian company that has resulted in significant operational savings.

Municipality of the County of Colchester

Description

1. Eight employees periodically were approved in 2017 to take Municipal cellphones with them out of Country. Prior to travel, approvals were obtained from the CAO to take phones out of Country.

Conditions

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

Reasons

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

Municipality of the County of Inverness

Description

1. Two (2) employees traveled outside of Canada with their mobile devices.

Conditions

1. Employees had their phones with them at all times.

Reasons

1. The mobile devices were necessary for employees to remain in contact with the Municipality and respond to email if necessary.

Municipality of the County of Kings

Description

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

Conditions

1. Access to information stored on municipal servers via mobile and laptop devices occurs via password protected accounts and information is accessed through the municipal portal. All devices and their use are subject to the municipal Network Policy and all protection of privacy regulations are followed when accessing and storing information on electronic devices. All data storage is within Canada; therefore, no restrictions are required on storage of data.

Reasons

1. Council and staff may be required to stay in contact with municipal operations while travelling outside Canada. The CAO, Mayor and Directors are expected to monitor emails in case of urgent matters or emergencies. In particular, the Mayor attended the 'International Network of Michelin Cities Conference' in France from November 29 to December 1, 2017 during which time he had remote access as outlined above.

Municipality of the County of Pictou

Description

1. Employees within the Municipality of Pictou County travelled outside of the country with their municipally 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 municipality's email system from their mobile devices, (iPhones, iPads and other smartphone devices).

Conditions

1. Mobile Devices are device password provisioned as well as securely managed and under the control of the Municipality'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.

Reasons

1. Employees or Elected Officials from the municipality may request to travel out of the Country with their municipally provided electronic devices. 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 within the Municipality if it is necessary for the user to travel with the device.

Municipality of the County of Victoria

Description

1. Municipal property owners living outside the country are sent property tax invoices. Occasionally there are email communications with them regarding their tax and/or water bills.

2. In the instance when the warden travelled outside Canada with an electronic device (iPad, iPhone), approval was granted beforehand.

Conditions

1. Email communication containing personal information is initiated at the request and with the written consent of the individual.

2. Devices are encrypted and password protected.

Reasons

1. This is necessary for property owners to communicate with the municipality and pay their bills.

2. Devices are required to allow for the warden to stay in contact with municipal operations.

Municipality of the District of Chester

Description

1. Remote Access via electronic devices such as iPhones, iPads and laptops. There were 4 instances in which staff members were approved to take electronic devices while traveling outside Canada. During this time staff had access to our email system from mobile devices.

Conditions

1. All devices are encrypted and password protected. AES-256 bit 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. Information stored on Municipal servers was accessed via electronic devices in the United States by two Councilors and three 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. Information stored on Municipal servers via mobile and laptop devices occurred via password protected accounts. All electronic devices are password protected, and information is accessed through the Municipal portal. All protection of privacy regulations are followed when accessing and storing information on electronic devices. Access to personal information by foreign entities is strictly forbidden. Should an access requested be received, the request must be reported to the Municipal Information Services Division immediately.

2. “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.

3. '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 and Hawaii.

2. The storage of information on ReCollect.net was necessary to conduct business in 2017.

3. The storage of information on Wrike.com was necessary to conduct business in 2017. 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 2017. 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 18 years.

Municipality of the District of Guysborough

Description

1. Being the Chief Administrative Officer, contact with the local offices and officials is required due to many ongoing files that are open at any given time. Data was only stored on smartphone and tablet. March 30th to April 6th, 2017 only.

2. Due to the large number of Economic Development files, the director was required to be in contact and was travelling on business to Houston, April 29th to May 2nd.

3. Due to the large number of Economic Development files, the director was required to be in contact and was travelling on business to Los Angeles, February 25th to 28th.

Conditions

1. Address book only accessed if needed. March 30th to April 6th, 2017 only.

2. Access only as required.

3. Access only as needed. February 25h to 28th.

Reasons

1. Travelling for vacation, but due to the large number of open files, contact was required via smartphone. March 30th to April 6th, 2017 only.

2. Due to the large number of Economic Development files, the director was required to be in contact and was travelling on business to Houston, April 29th to May 2nd.

3. Due to the large number of Economic Development files, the director was required to be in contact and was travelling on business to Los Angeles, February 25th to 28th.

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 their phones or laptop computers, which may contain personal information contained in e-mails and electronic files. During 2017, the following such requests were authorized:
    - One elected official
    - 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.

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 personal phone 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 Councilors, and both a laptops and mobile devices for staff while travelling outside of Canada.

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

Conditions

1. Mobile Devices (iPhone and iPad): Access to email is provided via the internet, mobile devices are required to have a passcode to access the device. Remote wipe capabilities are in place

for 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 of an SSL SharePoint site. 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, or accessed through the VPN connection.

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

Reasons

1. Council and Staff are required to stay in contact with municipal operations while travelling outside of the country.

2. The use of the VPN connection and password protected mobile devices allows that necessary level of access.

Municipality of the District of Yarmouth

Description

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

Conditions

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

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 urgent ongoing matters. Therefore, it is necessary for them to work remotely, where possible, in order to fulfill their responsibilities.

Property Valuation Services Corporation

Description

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

2. PVSC implemented Microsoft Office 365 in 2017. Personal information in Azure Active Directory and Office 365 Portal is stored in the U.S. because of Microsoft requirements. SharePoint data is currently being stored in a Microsoft data centre in the U.S. but PVSC has requested migration of the PVSC SharePoint data to Microsoft’s Canadian data centres, which has been guaranteed to be completed prior to the end of calendar year 2018.

Conditions

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

2. To access any personal information that is stored on servers in Microsoft data centres, PVSC workforce users must have authenticated credentials. Data in flight and in storage is encrypted and subject to Microsoft's privacy and security policies and safeguards, which meet industry standards. A privacy Impact Assessment is being conducted on the Microsoft Cloud Services Office 365 implementation.

Reasons

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

2. Office 365 provides modern, flexible, collaborative applications that meet PVSC's operational requirements. Office 365 has become the standard tool for other public bodies in Nova Scotia.

Region of Queens Municipality

Description

1. As part of emergency power restoration response one councilor was periodically out of Canada.

Conditions

1. All access to municipal mail accounts is restricted to users who must enter in the remote website address then enter a unique username and password

Reasons

1. In order to stay informed of municipal business it was necessary to retrieve Region of Queens Municipality emails on his personal phone.

Town of Amherst[21]

Description

1. Three Town of Amherst staff members travelled to the United States on personal time (vacation) in 2017 and had access to personal information (previous emails, email addresses) via their devices (iPhone, iPad or laptop). Prior approval to travel outside Canada with mobile devices was obtained from the CAO.

[21] Report includes Amherst Police Department Amherst Board of Police Commissioners and the Amherst Fire Department.

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

Conditions

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

2. EZ Labor- authentication is required through secure login password.

Reasons

1. Senior staff travelled for personal reasons; they were expected to monitor their business email in order to fulfill their job responsibilities during such absences. They were required to submit an application for the CAO' s approval to take any mobile devices outside Canada.

2. ADP's Global Privacy Policy requires that they protect our information and use it only for the purposes specified in our client contract with them; this assures that all ADP client data is handled in accordance with their policy, regardless of where it is processed.

Town of Bridgewater

Description

1. For the above noted calendar year, 2 employees travelled outside of Canada a total of 4 times and had accessed the Town of Bridgewater information via their smartphones. Both employees requested preauthorization to access his emails while away due to staffing issues and workload. In addition, 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. The Mayor tor the Town of Bridgewater also travelled outside of Canada one time and had accessed the Town of Bridgewater information via his phone, tablet and laptop.

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[22]

Description

1. CAO travelled to the USA for 2 days in 2017. IT and Admin made the decision that it was necessary for the CAO to be able to access email and utilize an iPhone while travelling.

Conditions

1. Devices are password protected and able to be remotely wiped in the event of an emergency.

Reasons

1. CAO is required to keep in contact with Council and Staff on important matters.

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.

Conditions

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

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.

[22] Report includes Kentville Police Department.

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

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.

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

Conditions

1. Mobile Devices (iPhone and iPad): Access to email is provided via the internet, mobile devices are required to have a passcode to access the device. Remote wipe capabilities are in place for administrator of IT network to remotely wipe any device that is lost or stolen. Also, unsuccessful passcode attempts will wipe device (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 or stolen. No municipal data (outside of email) is stored on the mobile device, only accesses through the SSL connection.

2. 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. Laptops can also access SharePoint through an SSL connection to SharePoint servers located in the Town of Middleton offices.

Reasons

1. Council and Staff are required to stay in contact with municipal operations while travelling outside of the country.

2. The use of the VPN connection and password protected mobile devices allows that necessary level of access.

Town of New Glasgow[23]

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.

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

Conditions

1. Mobile Devices have a device password provisioned as well as being 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 Agency 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. Processes have been put place in where the requesting user must fill out a form and submit to their department head/supervisor to request permission to travel outside of the Country with a Town owned 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 within the Municipality, if it is necessary for the user to travel with the device; such as senior staff or members of Council within the Municipality and senior officers within the Town's Regional Police Agency.

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.

[23] This includes the New Glasgow Police Service.

Town of Truro[24]

Description

1. A number of Town of Truro 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.

2. Access to Transient Data – Instances of municipal staff using cloud services to temporarily store files for the purposes of sharing with others and easily access data on multiple devices for meeting purposes. Services such as OneDrive, Dropbox and Google Drive are used from time to time to provide ease of access. This is not a permanent storage facility, but a quick method to share files with parties outside the municipal organization. Staff know not to 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). Access to municipal data on mobile devices outside of email is provided by the use of a VPN data

[24] This includes the Truro Police Service

connection. IT can revoke VPN access should the mobile device be lost of stolen. No municipal data (outside of email) is stored on the mobile device, or accessed through the VPN connection.

2. 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.

2. n/a

Town of Yarmouth

Description

1. Thirteen (13) Town of Yarmouth employees travelled outside of Canada with their Town issued smart phones. In each instance the employee requested and received approval to take their device. The employees had access to the Town of Yarmouth email system.

Conditions

1. All smart phones issued by the Town of Yarmouth are password protected. Remote access to the Town of Yarmouth email server from mobile devices or webmail is secured by a signed SSL certificate.

Reasons

1. When Town of Yarmouth staff or elected officials are travelling outside of Canada they are required to request and receive approval in order to take with them any mobile devices owned by the Town.

Foreign Access and Storage by Municipal Police

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

Amherst Police Department reported under the Town of Amherst. Annapolis Royal Police Department reported under the town of Annapolis Royal. 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. Truro Police Service reported under the Town of Truro. New Glasgow Police Service reported under the Town of New Glasgow.