FOI Privacy Breach Action Plan Department of Service Nova Scotia & Internal Services

Version: 1.3
January 2021

Please note: In June 2019, the Department of Internal Services was merged to create the Department of Service Nova Scotia and Internal Services.

NOVA SCOTIA

Since 2015, the provincial government has supported the values of freedom of information and the protection of the personal information of Nova Scotians through its shared services approach to administering the Freedom of Information and Protection of Privacy Act. This effort demonstrates government's commitment to supporting the values outlined in the Act.

The Freedom of Information Requestor and Disclosure Portal was intended as another example of balancing these core values. It improved and simplified the administrative processes for people who were searching for information from the province and made non-sensitive information that had already been disclosed more widely available through public access. What was learned in April of 2018, and is outlined in the review reports, is that despite the best of intentions this site was the source of the unauthorized disclosure of the information of many Nova Scotians.

The Department of Service Nova Scotia & Internal Services thanks the Auditor General and the Privacy Review Officer for their investigations and reports. We accept all of their recommendations and have developed this action plan to achieve the objectives outlined in their reports. We fully recognize and acknowledge the role government had in this incident and are committed to making the changes needed to better protect the information of Nova Scotians.

Key Terms Defined

AG	Auditor General
ARB	Architecture Review Board
CERT	Computer Emergency Response Team
COBIT	Control Objectives for Information and Related Technologies
HRP	Halifax Regional Police
ICTS	Internal incident review by Information Communications and Technology Services
NIST	National Institute of Standards and Technology
OWASP	Open Web application Security Project
PIA	privacy impact assessment
PMBOK	Project Management Body of Knowledge
QA	quality assurance
RO	Privacy Review Officer
SMU	Saint Mary's University
SANS	SysAdmin, Audit, Network and Security
TRA	threat risk assessment

Review	Recommendation/ Observation	Response to Recommendation/ Observation	Planned Activity	Current Status
AG1	The Department of Internal Services should conduct comprehensive risk assessments for IT projects prior to implementations.	The department accepts this recommendation. The level of project risk and complexity will vary based on the type of project; therefore, risk assessments and risk management will also vary based on the type of project. Project risk management practices including TRA and PIA processes have been and will continue to be enhanced and implemented. To support new initiatives and ongoing operations we have recently developed and communicated to staff an overview/guide describing the proper timing and execution of TRAs and PIAs. In addition, measures will be taken to increase awareness and invest in training and awareness for project team members, managers and client departments in general, to ensure adoption of risk management practices, including risk registers and mitigation strategies in alignment with industry best practices such as Project Management Book of Knowledge and frameworks such as Control Objectives for Information Technology and National Institute of Standards and Technology for Cybersecurity.	**Activity 1 Objective:** to address website design – revisit policies, processes, standards and guidelines associated with website design and implementation. **Activity 2 Objective:** to address the approach to risk assessments-Assess and follow an incremental multi-year approach to adopt risk frameworks from COBIT 2019, NIST and project management best practice PMBOK, organization structure changes, role clarity, new QA process, creation of policies, processes, standards, guidelines and checklists etc. **Activity 3 Objective:** to address risk assessments – update the existing processes and policies, educate and communicate for TRAs and PIAs.	***Update January 2021:*** **Activity 1** ***Completed:*** *A web technology security policy – with updated standards, processes, intake process, web security guidelines, and updated secure websites creation process (including mandatory vulnerability scan before go-live), this work aligns with industry best practices from CERT, NIST, OWASP, SANS. The above has been communicated and is being enforced. Wide Area Network (WAN) Security Policy has been updated.* **Activity 2** ***Completed:*** *ICTS Executive approved adoption of COBIT 2019; COBIT 2019 Foundation Certificate Program training sessions have been held in April, May, and June of 2019 with staff participation from Government and Health Sector. Developed a roadmap for implementing an IT Risk Management Program; program implementation has been initiated and ongoing.* **Activity 3** ***Completed:*** *Comprehensive Guide to Writing a PIA was completed and communicated to project managers; developed and implemented an integrated Privacy and Security Risk Assessment process.*
AG2	The Department should clearly define the scope of responsibilities of the Architecture Review Board and ensure stakeholders clearly understand what IT projects should be submitted. The scope should include new IT systems or changes to existing systems and should require a full scope of documentation and testing.	The department accepts this recommendation. A review of the current scope, mandate and supportive processes is being performed, and where appropriate, improvements and enhancements will be implemented, communicated and enforced. Project assessment considerations will include scalability, timing, intake processes and documents, required output, and supportive governance structures, with a focus to ensure new IT systems and changes to existing systems are examined at the proper governance levels and at the right time.	**Activity 1 Objective:** review the scope of responsibilities of the ARB – there were will a number of areas that will be reviewed – scope of the mandate, membership, roles, processes, types of projects review, relationship to other committees, e.g. Standards Committee, alignment to COBIT 2019, etc.	***Update: January 2021:*** **Activity 1** ***Completed:*** *ARB's scope of responsibilities defined in an updated Terms of Reference document including three approval gates with clearly communicated requirements for IT projects.*

Review	Recommendation/ Observation	Response to Recommendation/ Observation	Planned Activity	Current Status
AG3	The Department should establish criteria to ensure adequate project management expertise is in place for all projects. This criteria should be documented, communicated and put into practice in managing teams.	The department accepts this recommendation. A resource fulfillment process for assigning project team members, including project managers, will be developed and implemented, and will include identification of key engagement criteria. It will be used for matching project team members with the appropriate skills and experience to IT projects as well as to support project managers in gaining experience and skills to progress through their careers.	**Activity 1 Objective:** Address project management processes observed in the FOIA project – Overview of project management practices and processes and develop a plan to address deficiencies, communicate and educate. **Activity 2 Objective:** strengthen project management practices. Including but not limited to, address the role of the project sponsor, institute a quality assurance process for project documentation, assess project management skills – provide education and support. **Activity 3 Objective:** to address completeness of Project Charters. Establish a QA process to assess project charters with a focus on risk identification and mitigation strategies within the charter.	***Update January 2021:* Activity 1** ***Completed:*** *Project lessons learned documented and communicated; all PMOs were consolidated into one corporate PMO effective April 1, 2019.* **Activity 2** ***Completed:*** *Developed and implemented PMO Standard Operating Procedures (including Project Manager assignment process). NSDS's delivery model will be reviewed and further refined as part of the ongoing work to consolidate the departments of SNS and IS.* **Activity 3** *Completed: Updated Project Management templates (including Project Charter); a process for reviewing and approving a Project Charter exists; implemented a Risk Register Framework and a process for ongoing review of project risk registers.*
AG4	The Department should establish a process to ensure and document vendor compliance with contract terms at all stages of a contract.	The department accepts this recommendation. With the creation of Shared Services, more robust processes are being put in place to manage and administer IT vendor compliance starting with major contracts and vendor relationships. Contracting terms and process associated with compliance are stronger in newer contracts. An analysis of vendor relations and contract governance capacity has been completed. Work will continue to ensure processes are put in place to monitor compliance with contract terms.	**Activity 1 Objective:** to strengthen contractual oversight of vendors. An assessment of the current capacity for vendor oversight, contract administration and contract management will be undertaken and an action plan will be developed.	***Update: January 2021:* Activity 1** ***Completed:*** *Assessment of capacity for vendor oversight.* **In Progress:** SNS-IS is developing ongoing processes to monitor compliance with contract terms.
AG5	The Department should ensure contracts with vendors include service expectations and financial obligations.	The department accepts this recommendation. New contract templates have already been established that include many standard terms and conditions including explicit service level expectations and failure consequences and new security and privacy terms and conditions. Contract terms and conditions will continue to evolve as the IT industry evolves and will be developed to ensure the proper requirements are made to the various types of IT systems.	**Activity 1 Objective:** to strengthen contracting processes. Actions associated with AG Recommendation 4 will also ensure contracts include service expectations and financial obligations. Activities aligned with recommendation will be addressed as ongoing continuous improvement. Structure, role clarity associated with contract management and contract administration, as well as, the development of contracting guidelines will enhance contract due diligence. **Activity 2 Objective:** to ensure updated policies and update terms associated with cybersecurity and privacy requirements are included in contracts. Activities will include updating Contract Terms for Privacy and Security at both the RFP and contracting stage. (note this is a continuous improvement activity).	***Update: January 2021:* Activity 1&2** ***Completed:*** *Updated and improved privacy and cybersecurity obligations contract schedules for all new IT system procurements and contracts. Newer contracts already have improved terms, expectations, and obligations (continual improvement activity).* (Actions being undertaken to address AG recommendation #4 will further support this recommendation).
RO1	Strengthen privacy leadership in government and due diligence in the privacy impact assessment process.	The department accepts this recommendation as per the letter of response to the Review Officer in January 2019.	**Activity 1 Objective:** strengthen privacy leadership. Actions will include enhancing and growing the privacy team in IAP and well as the creation of corporate policies and training. **Activity 2 Objective:** to continue to strengthen and enhance the privacy impact assessment process. Activities to support this objective include, but are not limited to, education and training, quality assessments, PIA and TRA follow-up process, updated documentation. (Note: this is a continuous improvement activity).	***Update: January 2021:* Activity 1** ***Completed:*** *Increased staff within the privacy team at IAP Services; implemented a Privacy Framework and Corporate Privacy Policy; launched mandatory online awareness training (7886 employees have taken this training effective Fall 2020); privacy impact assessment tools, resources and guidance documents have been completed and rolled out; all members of Privacy Program and four staff in the Access Program completed IAPP Privacy Certification in September 2019; a Privacy Forum to facilitate knowledge sharing among privacy professionals was created in November 2019 and has convened three times to date.* **Activity 2** *Ongoing: Strengthening privacy impact assessment process, analysis and monitoring of risks.*
RO2	Take immediate steps to contain the breaches that resulted in the download of 618 documents containing personal information to a private computer that has not been secured by the Department (breaches #2-#12).	The department accepts this recommendation as per the letter of response to the Review Officer in January 2019.	**Activity 1 Objective:** Containment for Breach #1. Action the department will continue to work with HRP regarding the containment of the data on devices seized by the HRP. **Activity 2 Objective:** Containment for Breaches #2–12. Work with HRP and SMU regarding containment. **Activity 3 Objective:** Containment. Continue to scan the internet for the next 12 months to determine if any of the documents have been shared or posted.	***Update January 2021:* Activity 1** ***Completed:*** *HRP has secured the devices.* **Activity 2** ***Completed:*** *All documents related to breaches #2-12 have been contained.* **Activity 3** ***Completed:*** *Conducted three searches of the internet to determine if downloaded documents are available – none were found.*

Review	Recommendation/ Observation	Response to Recommendation/ Observation	Planned Activity	Current Status
RO3	Take all reasonable steps necessary to notify individuals affected by the download of the 618 documents containing personal information (breaches #2-#12).	The department accepts this recommendation as per the letter of response to the Review Officer in January 2019.	**Activity 1 Objective:** Containment. Outcome of the activities from RO Recommendation #2 will determine further action to be taken on this recommendation. Refer to Review Officer Report Footnotes 48 and 53.	***Update January 2021:*** **Activity 1** ***Completed:*** *A risk assessment was conducted to confirm the requirement of notifying affected individuals; the risk was determined to be low, therefore individuals were not notified.*
RO4	Conduct an internal post-incident review as an aid to ensuring that the Department fully understands the causes of these breaches and has identified all reasonable steps necessary to prevent future similar errors.	The department accepts this recommendation as per the letter of response to the Review Officer in January 2019.	**Activity 1 Objective:** Conduct a formal process to access learning — causes and steps to prevent similar errors in the future. Actions include engaging an external subject matter expert to guide the lessons learned activity. **Activity 2 Objective:** Conduct other internal and vendor assessments of this incident. **Activity 3 Objective:** to be open and transparent in tracking progress for improvements. Action is the creation of an Action Plan that will be shared publicly.	***Update January 2021:*** **Activity 1** ***Completed:*** *Deloitte engaged in November 2018 to conduct lesson learned. Final report received in January 2019. All ISD staff have had communication about these reports and key staff involved in this incident have been directed to read the report.* **Activity 2** ***Completed:*** *Assessment on May 15, 2019 with CSDC and Unisys, and ICTS completed lessons learned on May 17, 2019* **Activity 3** ***Completed:*** *Second version of an action plan published in August 2019; plan to be updated as implementation proceeds.*
RO5	Conduct an inventory of technology solutions, devices and applications across government and rate their vulnerabilities beginning with systems storing the most valuable personal information and/or having the highest risk.	The department accepts this recommendation as per the letter of response to the Review Officer in January 2019.	**Activity 1 Objective:** to have inventories of systems that contain sensitive personal information. Action: Continue to inventory and protect systems at various levels in various ways. **Activity 2 Objective:** Rate vulnerabilities associated with systems that contain sensitive information. Actions will include on a go forward bases strong PIA and TRA policies, processes, and practices. For existing systems enhanced security scanning will continue — continuous improvement activity.	***Update January 2021:*** **Activity 1** ***Completed:*** *Information Asset Register established, identifying data sets that contain personal information; established an inventory of projects that plan to collect, use and disclose personal information and determine PIA requirements and status; developed an inventory of personal devices and assessed risk related to the personal information on them in Government; developed an inventory of network devices and assessed risk related to the personal information on them; developed an inventory of applications that include personal information. Ongoing work to mitigate the risks associated with personal/network devices, and applications.* **Activity 2** ***Completed:*** *Projects are using PIAs and TRAs for identifying vulnerabilities and documenting risks; an integrated Privacy and Security Risk Assessment process describing key stakeholders and activities was developed and implemented.*
RO6	Clarify and strengthen the role of the Architecture Review Board.	The department accepts this recommendation as per the letter of response to the Review Officer in January 2019.	**Note:** This recommendation aligns with Recommendation #2 from the AG. Refer to the activities recorded in AG2 above.	Refer to the Status reported in AG Recommendation #2 above.