



Privacy Breach Reporting Form

For Ministerial Public Body Employees

First name	Last name	Position
IMS		
Branch/unit	Phone	Email
Caitlin Moorcroft		
Name of Public Body Designated Privacy Officer		

Complete the following fields. Select all that applies:

- | | |
|--|--|
| <input type="checkbox"/> Unauthorized use | <input type="checkbox"/> Unauthorized disclosure |
| <input checked="" type="checkbox"/> Loss or theft of information | <input type="checkbox"/> Loss or theft of a device |
| <input type="checkbox"/> Unauthorized disposal | |

Date of suspected breach: Dec 20, 2022

Date breach was discovered: Dec 20, 2022

Location of suspected breach: IMS Employee Laptop

Number of individuals affected: 1

For assistance completing this form, please see the [Guidance for Reporting a Suspected Privacy Breach](#).

1) Describe the circumstances of the suspected breach and how it was discovered. Please provide a detailed description including any systems that may be involved. Do not include any personal or identifiable information.

Please select all fields related to the incident on **Appendix A:**

Between 9:50 AM and 10:20 am, A hacker identified themselves as a Microsoft representative and tricked an employee into providing access to their computer by saying that a number of trojans were on the computer, identified it as high risk and needing to be resolved urgently.

The employee allowed access and the hacker began to scan files. She became concerned and called ICT Tech Support within approx. 20 minutes, IT advised the employee to immediately shut down the Laptop and bring it to their technicians.

After shutting down the laptop the employee received several phone calls and a voice message. The employee did not answer or respond to any of these.

After restarting the new laptop the employee reviewed their outlook sent items and noticed an email that she did not write was sent from their email address at 10:00 am on December 20.

The employee immediately changed all passwords and it appears the incident has been isolated. The laptop remained with our ICT security system specialist for full investigation for several months. That investigation is concluded and there is no risk of significant harm identified.

2) List the immediate containment actions you have taken to prevent further access:

Shut laptop down and provide it to IT immediately upon being made aware of breach.

The compromised laptop was replaced by brand new laptop and compromised laptop provided to the ICT security systems specialist.

All passwords were changed immediately upon start-up of the new laptop.

Ongoing monitoring for any unusual activity.



DESIGNATED PRIVACY OFFICER BREACH REPORTING FORM

1 Accountability

Name of Public Body:	Department of Finance
Assessment by:	Linda Klippert
Email/Contact:	Linda.Klippert@yukon.ca
Date assessment completed:	2023/01/26
Date breach was discovered:	2023/01/18
Location of Assessment:	Department of Finance

2 Containment of Information

2.1 Has there been a breach involving personal information?

Under the ATIPP Act, [Appendix C] a Privacy Breach is defined as "in respect of personal information, means the theft or loss of, or unauthorized use, disclosure or disposal of, the personal information." Only the Department of Finance has the authority to collect and use Social Insurance Numbers as per the Income Tax Act [Appendix F] and the Financial Administration Act. (FAA) [Appendix D]. The authority is only for collection and use to produce T4's and T4A's within the Department of Finance. The disclosure of the SIN's from the Department of Finance to other Departments is unauthorized.

YES, there has been a breach.

2.2 List the immediate containment actions, as well as any subsequent containment actions.

On January 18, The Department of Finance employee asked all recipients to delete the information from the document and verify that it had been deleted. 26 of the 34 recipients confirmed verbally the email had been deleted, 8 were sent an email to delete, 4 of which were out of office. Upon receiving the Privacy Breach Report Form for Employees [Appendix B] on January 20, the Designated Privacy Officer sent an email to all recipients of the erroneous email to delete said email and the attachment, including any saved copies and to provide confirmation in writing once complete. One Department had already completed their work and saved the document to their record storage. They have confirmed the deletion of the SIN numbers. As of January 25, all copies of the document have been deleted with written confirmation from all 34 recipients provided to the DPO.

3 Risk of significant harm analysis

3.1 What is the cause of the breach?

This situation relates to the payments made to individuals by Departments, for which T4 and T4A's need to be created. Each Department has the ability to pay for services rendered. Once a payment is required, the Department identifies if a Vendor Request Form [Appendix L] needs to be completed

and sends the form to the Department of Finance, Accounts Payable. A Vendor ID number is then created and entered by A/P into the main Financial Application used for payroll. (This system is also referred to as FM/FMIS or Masterpiece) All Departments have access to all vendors but can only view the transactions that occurred within their Department. This vendor form states that all individuals need to complete a SIN Form for Social Insurance Number **[Appendix K]** which is sent directly to Department of Finance from the individual.

All Departments are to request the SIN from their vendors using the SIN Request Form for Social Insurance Number which is mailed directly from the individual to the Department of Finance for the direct collection and use of the information.

To ensure correct coding, and the T4/T4A is mailed to the correct individual, the Department of Finance is required to verify the cheque amount, Vendor ID, Account ID, Payment ID, Issue and Cleared date of the payment, Name, mailing address and brief description of services provided with each Department to ensure accuracy.

As requested in the Memo dated January 3, 2023 **[Appendix M]** sent by the Comptrollers Office to all Departments, each Department was asked to email a list of vendors who have been identified as requiring a T4/T4A for Honoraria, Awards, Scholarships and Bursaries, Relocation and Other Allowances, Cash Gratuity on Death and other Recognitions such as gift cards to the Department of Finance, Financial Accounting. These payments are taxable and therefore a T4/T4A must be produced.

With this information, a spreadsheet is generated by Department of Finance, Financial Accounting from FM which includes the Vendor ID and Name, mailing address, SIN and multiple other unique identifiers. Prior to the removal of the SIN, this document was sent directly to each Department.

When an employee of Financial Accounting was reviewing the spreadsheet on January 18 it was discovered that the SIN number was not removed from the document before being emailed. This is when the breach was identified,

3.2 How many individuals are affected?

2,047

3.3 What is the sensitivity of the personal information?

Highly Sensitive

3.4 What is the possibility that the personal information is, has been or will be used or disclosed in an unauthorized manner?

There is a low possibility the information will be used in an unauthorized manner as all Employees of YG agree to the Oath of Office under Yukon Government's General Administration Manual Policy 3.16 **[Appendix N]** when accepting employment.

The time between when the information was disclosed and fully contained was 10 days.

3.5 How much time elapsed between the occurrence of the privacy breach and the determination that it occurred?

The email was sent January 11, 2023 and it was identified January 18, 2023. 6 Working days.

3.6 What is the type of relationship, if any, between affected individuals and any person who may have used, or to whom may have been disclosed, the personal information?

The relationship is of a professional capacity. The SIN numbers were of individuals that provided a service to YG during the 2022 year. Those who received the SIN's in error were all designated employees in Finance Branches of other Departments who are responsible for personal information.

3.7 What measures have been or are being implemented to reduce the risk of significant harm to the affected individuals?

The information has been 100% contained.

3.8 If the personal information has been lost, stolen or disposed of, has any of the personal information been recovered?

N/A

3.9 Is any other information available that assists in the determination of risk of significant harm to affected individuals?

3.10 Outcome – is a risk of significant harm to affected individuals present?

SIN's are considered highly sensitive personal information [Appendix A]. The Department of Finance is the only Public Body that has the authority to collect and use this information. There is no authority to disclose to any other Department.

Along with the SIN's, the spreadsheet contained Name, address, payment amounts, and other unique identifiers. There is a risk of identity theft and as such, meets the threshold of significant risk of harm to affected individuals.

NOTE: If you determine that there is a risk of significant harm, you MUST notify the affected individuals, the Head of the public body, and the Office of the Information and Privacy Commissioner.

4 Notification

4.1 Internal Notifications

Identify the individual(s) notified and the date of notification. Only individuals that can reasonably be determined to have a legitimate need-to-know should be informed of the breach. The affected program's director should be notified of the breach. In collaboration with the director, you will determine what member(s) of management, if any, should be notified. For example, Director of Communications, ADM, and/or DM.

Position	Name of Individual and date of notification
Director of Communications	Eric Clement Jan 18, 2023
Comptroller (program Director)	Ralph D'Alessandro Jan 18, 2023
Designated Privacy Officer	Linda Klippert Jan 19, 2023
Deputy Minister	Scott Thompson Jan 23, 2023

4.2 Will affected individuals be notified in cases where risk of significant harm is not present? If not, why not?

All affected individuals will be notified.

6 Prevention

6.1 Describe any physical security safeguards proposed or already in place.

Documents are kept in a secure Department (employee swipe card required to enter) and filing cabinets are locked.

6.2 Describe any technical security safeguards proposed or already in place.

Records containing PI will be sent via Secure File Transfer or will be encrypted in accordance with Yukon Governments' Guidance for Protecting Government Information [Appendix H] and Guidance on Safeguarding Information Assets. [Appendix G]

6.3 Describe any administrative security safeguards proposed or already in place.

Review Department Policies and update or develop to meet the Guidance for Protecting Government Information.

The reference manual for Financial Accounting was immediately updated to include the removal of SIN numbers from the spreadsheet before being sent to other Departments.

The process for amalgamating the spreadsheet and the information that is produced from the payroll system is being reviewed. Specifically, identifying if the SIN number is required on the spreadsheet.

6.4 What other internal improvements to processes, systems, policies, and any other actions to mitigate recurrence are recommended? What is the timeline for implementation?

Recommendation #1: All Department of Finance Employees complete ATIPP ACT Level 1- Introduction to the ATIPP Act and Level 2 Protection of Privacy Training on YG Learn as outlined in the Corporate Training Policy for Employees [Appendix J].

Timeline for Completion: June 30, 2023

Recommendation #2: Update onboarding process for new Department of Finance employees. Include these documents to orientation which provide direction on encrypting all sensitive documents including those containing personal information prior to emailing.

- [Privacy Management Policy \(GAM 2.27\)](#)
- [Guidance for Protecting Government Information.](#)
- [Guidance on Safeguarding Information Assets](#)

Timeline for Completion: Immediately

Recommendation #3: Financial Operations review current process around collection/use and destruction of social insurance numbers and T4/T4A generation and disposition. Identify relevant legislation, current risks, implement mitigations and update processes. Revise procedures and communicate changes as required.

Timeline for Completion: July 31, 2023

4 SUBMISSION

Upon completion of report, print and disseminate recommendations to all required parties.

Linda Klippert

Designated Privacy Officer Signature

February 3, 2023



Date

When **risk of significant harm** exists, you **must** forward a copy of this completed breach report to:

- The Office of the Information and Privacy Commissioner
- The Access and Privacy Officer (ATIPP Office) when the breach involves a Ministerial public body

APPENDICES:

Include any supporting documentation as appendices to the breach report.

Appendix	Name of Document
A	Personal Information and Personal Health Information Listing
B	Privacy Breach Report Form for Employees
C	Access to Information and Protection of Privacy Act (yukon.ca)
D	Financial Administration Act
E	Financial Administration Manual
F	Income Tax Act
G	Guidance on Safeguarding Information Asset
H	Guidance for Protecting Government Information.
I	Privacy Management Policy (GAM 2.27)
J	 Corporate Employee privacy tra
K	SIN request form for Social Insurance Number
L	Vendor Request Form
M	 2023 T4-T4A memo.pdf
N	GAM 3.16- Employee Documentation, Oaths and Personal Information

APPENDIX A:

PERSONAL INFORMATION AND PERSONAL HEALTH INFORMATION LISTING

Note: This is not an exhaustive list of personal information and/or personal health information.

Identification and Contact Information		Unique Identifiers		Financial Information	
Name or alias	x	User name		Real estate	
Address	x	Password		Tax information	x
Residency		Unique identification number		Credit history	
Home or cell phone		Social insurance number	x	Income	x
Email address		Case file number		Expenditures/liabilities	
Gender		Electronic signature		Bank accounts	
Nationality		Yukon Health Insurance number		Credit or debit card numbers	
Place of Birth		Employee ID		Expiration dates	
Date of Birth		Driver's license number		Magnetic stripe data	
Age		Other (please specify)		PIN or security code	
Marital status				Insurance information	
Number of dependents				Legal status (judgements, injunctions, proceedings)	
Signature				Other (Please specify)	x
Other (Please specify)				Vendor ID	
				SIN	x
Physical Characteristics		Employment Information		Health Information	
Skin colour		Name of Employer		Health care status or diagnosis	
		Employment history			
		Employment references			
		Experience/training			
		Information generated during recruitment or selection process			

Test results or medical images	
Medications	
Diagnosis	
Disability	
Sensitive Data	
Religious views or affiliation	
Philosophical beliefs	
Political views	
Union membership	
Health information	
Genetic information	
Data on sexual life/preferences	
Ethnic background	
Criminal history	
Information about vulnerable person	
Other (please specify)	