Rainy River District Social Services Administration Board

Appendix B
Privacy Breach CHECKLIST

INCIDENT DESCRIPTION	
Date of Incident:	Date Incident Discovered:
How was it Discovered:	
Location of the Incident:	
Cause of the Incident:	

Step 1: CONTAINMENT/ASSESSMENT	
Person designated as Lead Investigator:	Date Assigned:
Date Breach was contained:	Time Contained:

Measures taken to contain the breach: *(recovery of information, computer system shut down, locks changed, etc.)*

List names of *Breach Response Team*:

Are there internal and/or external persons to be advised of the breach? ❑ Yes ❑ No

- List Names/Organizations who need to be advised:

Does the breach appear to involve theft or criminal activity? ❑ Yes ❑ No

- If yes, have the Police been notified? ❑ N/A ❑ Yes ❑ No

List measures taken to ensure evidence that may be necessary to investigate the breach is not destroyed:

Step 2: EVALUATE THE RISKS

a) What personal information was involved?

❑ Name ❑ Address ❑ SIN ❑ Financial ❑ Medical ❑ Other: _____

Details:

What form was it in? ❑ Paper Records ❑ Electronic ❑ Other:

Details:

What physical/technical security measures were in place at time of incident: (*locks, alarms, encryption, passwords)*

Step 2: EVALUATE THE RISKS *(cont.)*

b) What was the cause and extent of the breach?

Is there a risk ongoing breaches or further exposure of the information? ❑ Yes ❑ No

- If yes, explain:

Can the personal information be used for fraudulent or other purposes? ❑ Yes ❑ No

- If yes, explain:

Was the information lost or stolen? ❑ Lost ❑ Stolen ❑ Other: _____

If stolen, can it be determined whether the information was the target of the theft:

The personal information been recovered?

Is this a systemic problem or an isolated incident?

c) How many individuals have been affected by the breach and who are they?

- **List who's been affected:** *(eg. employees, contractors, public, clients, tenants, service providers, organizations)*

d) Is there any foreseeable harm from the breach?

- **What harm to the individuals could result from the breach:** *(eg. security risk, identify theft, financial loss, loss of business or employment opportunities, physical harm, humiliation, damage to reputation, etc.)*

Do you know who has received the information and what is the risk of further access, use or disclosure?

What harm to our organization could result from the breach? *(eg. loss of trust, loss of assets, financial exposure, legal proceedings, etc.)*

What harm could come to the public as a result of notification of the breach? *(eg. public health or safety. etc/)*

Step 3: NOTIFICATION

a) Should affected individuals be notified?

Consider the following before making a decision:

- What are the reasonable expectations of the individuals concerned?
- What is the risk of harm to the individuals? Is there a reasonable risk of identify theft or fraud?
- Is there a risk of physical harm? Is there a risk of humiliation or damage to their reputation?
- What is the ability of the individual to avoid or mitigate possible harm?
- What are the legal and contractual obligations of the organization?

Should affected individuals be notified: ❑ Yes ❑ No

- If you decide that affected individuals do not need to be notified, note your reasons:

b) If affected individuals are to be notified, When and How will they be notified and who will notify them?

❑ Phone ❑ Letter ❑ Email ❑ Letter ❑ In Person ❑ Media ❑ Website

❑ Other:

Are the services a third party required? ❑ No ❑ Yes, List:

Person Responsible for Notification:	Title:

If law enforcement authorities are involved, does notification need to be delayed to ensure that the investigation is not compromised? ❑ Yes ❑ No

Details:

c) What should be included in the notification?

Be careful to limit the amount of personal information disclosed in the notification to what is necessary. Depending on the circumstances, notifications c*ould* include some of the following:

- Information about the incident and its timing in general terms.
- A description of the personal information involved in the breach.
- A general account of what your organization has done to control or reduce the harm.
- What your organization will do to assist individuals and steps individuals can take to reduce the risk of harm or further protect themselves.
- Sources of information designed to assist individuals in protecting against identity theft.
- Contact information of a department or individual within your organization who can answer questions or provide further information.
- Whether your organization has notified a Privacy Commissioner's Office.
- Additional contact information to address any privacy concerns to your organization.
- Contact information for the appropriate privacy commissioner(s).

Step 3: NOTIFICATION *(cont.)*

d) Are there others who should be notified about the breach?

❑ Privacy Commissioners Office ❑ Police ❑ Insurers ❑ Professional Bodies ❑ Regulatory Bodies
❑ Credit Card Companies ❑ Financial Institutions ❑ Credit Card Reporting Agencies
❑ Third Party Contractors ❑ Internal Business Units ❑ Staff Association ❑ Union VP ❑ Other
Details:

Step 4: PREVENTION OF FUTURE BREACHES

What *short-term* steps do we need to take to correct the situation? *(eg. staff training, policy review, etc.)*

What *long-term* steps do we need to take to correct the situation? *(eg. policy development, internal audit, etc.)*

Completed by Lead Investigator *(print)*:	Job Title:
Signature of Lead Investigator:	Date: