Newfoundland Labrador

Labour Relations Board

Effective 4 March 2022

POLICY CIRCULAR
PROCEDURE FOR ADDRESSING AND CONTAINING PRIVACY BREACHES

At its meeting of 4 March 2022 the NL Labour Relations Board ("Board") adopted the below Policy in relation to the procedure for addressing and containing privacy breaches.

PURPOSE

The purpose of this Policy and Procedure is to provide a consistent and effective approach to the investigation, management and containment of privacy breaches involving personal information.

INTRODUCTION

A privacy breach involves the collection, use, or disclosure of personal information in contravention of the *Access to Information and Protection of Privacy Act, 2015* (the "*Act*").

A privacy breach occurs when personal information is inappropriately collected, used or disclosed. A privacy breach also occurs when information is lost, stolen, mistakenly disclosed or accessed without a legitimate work purpose.

The *Act* makes it mandatory for all public bodies, including the Labour Relations Board (the "Board") to report all privacy breaches to the Office of the Information and Privacy Commissioner (the "OIPC").

This Policy and Procedure will be applied by the Board when a privacy breach occurs.

PROCEDURE: STEP 1 (PRELIMINARY ASSESSMENT AND CONTAINMENT)

A staff member of the Board who becomes aware of a possible breach of privacy involving personal information in the custody or control of the Board will immediately seek to retrieve the personal information in accordance with the Board's Remediation Plan for Privacy Breaches. The staff member will then inform the C.E.O. of the Board, the Deputy C.E.O. and the Board's ATIPP Coordinator.

Once a breach of personal information has been confirmed the C.E.O. or designate will identify the cause, extent and risks associated with the privacy breach. The C.E.O. or designate will also take immediate action to retrieve the personal information, contain the privacy breach and prevent any further privacy breaches of a similar nature. In the event of a cyber breach, the C.E.O or designate wil request the immediate shut down of the system that was privy to the breach, will revoke or change computer access codes or correct weaknesses in physical or electronic security.

PROCEDURE: STEP 2 (NOTIFICATION)

The C.E.O. or designate will notify the Chairperson of the Board (the "Chairperson") and the Deputy Minister of the Department of the privacy breach.

The Chairperson of the Board will provide notification of the privacy breach to the OIPC and the Access to Information and Protection of Privacy Office in accordance with the *Act*, using the Privacy Breach Reporting Form (https://www.oipc.nl.ca/pdfs/PrivacyBreachReportingForm.pdf).

The Chairperson, in consultation with the C.E.O., will notify the affected individual(s), including any union or employer (if applicable), concerning the privacy breach, in accordance with the Act. The Chairperson, in consultation with the C.E.O, will provide the notification as soon as possible and provide as much information as possible during the notification (i.e. date of breach, manner of breach, information disclosed, steps taken to eliminate or contain the harm, contact information for the OIPC). The Chairperson in consultation with the C.E.O. may also contact the police concerning the privacy breach.

PROCEDURE: STEP 3 (EVALUATE THE RISK)

The Board's ATIPP Coordinator, in consultation with the C.E.O., will evaluate the risks associated with the privacy breach. The assessment of risk will be used as part of the Board's Remediation Plan for Privacy Breaches. The following factors will be considered in assessing the risks:

(i) Personal Information - identify the personal information that has been breached; the more sensitive and confidential the information the higher the risk;

(ii) Cause and Extent of the Breach – identify the cause and extent of the breach and whether there is a risk of ongoing or further disclosure of any personal information; any further steps to minimize the potential harm should be put in place;

(iii) Number of Individuals – identify the number of individuals affected by the privacy breach;

(iv) Foreseeable Harm from the Privacy Breach – identify what potential harm will result to affected individuals from the privacy breach (i.e. security risks, identity theft or fraud, loss of business or employment, damage to reputation);

(v) Harm to the Board and Department – identify the potential for reputational and financial damage to the Board and the Department (i.e. loss of confidence in Board operations, loss of assets and possible financial exposure);

(vi) Harm to the Others – identify the harm that could result to third parties or the public resulting from the privacy breach;

(vii) Extent of Relationship – determine (if possible) whether a relationship exists between the unauthorized recipient(s) and the subject of the breach. That is, evaluate if the recipient is a trusted and known entity who can reasonably be expected to return the information in question without disclosure or use;

(viii) Security of Information – determine whether the personal information was adequately encrypted, anonymized or otherwise made difficult to access;

(ix) Nature of Breach – determine whether the breach can be deemed a systemic problem or an isolated incident;

(x) Assessment - assess what steps, if any, have already been taken to mitigate the harm resulting from the privacy breach; and

(xi) Form – the ATIPP Coordinator will complete the attached Privacy Breach Form (Schedule A) and deliver it to the C.E.O.

PROCEDURE: STEP 4 (MITIGATION AND PREVENTION)

The Board's ATIPP Coordinator, in consultation with the C.E.O., will review the circumstances that caused the privacy breach and the Board's follow-up to the privacy breach.

The ATIPP Coordinator, in consultation with the C.E.O., will identify any steps that can be taken in the future to improve the Board's investigation, management and containment of privacy breaches.

The ATIPP Coordinator, in consultation with the C.E.O., will also identify any potential training or education that the Board could use in the future to better prevent or manage privacy breaches. A privacy breach prevention plan should be considered depending on the significance of the privacy breach and whether it was a systemic breach or an isolated incident. The plan may include the following:

- A security audit of both physical and technical security;

- A review of policies and procedures and any changes to reflect the lessons learned from the incident and investigation (eg. Security policies, privacy policies, record retention policies, etc);

- A review of employee training practices; and

- A review of interactions with other professional bodies, individuals, and other regulatory authorities.

The resulting prevention plan may include a requirement for an audit at the end of the process to ensure it has been fully implemented.

PROCEDURE: STEP 5 (PRIVACY BREACH REPORTING)

The ATIPP Coordinator, in conjunction with the C.E.O., will confirm that the OIPC has been given proper notice of the privacy breach, in accordance with the *Act*.

The ATIPP Coordinator, in conjunction with the C.E.O, will also ensure that reporting of the privacy breach is provided in the Board's Annual Report. This will be coordinated, as necessary, through the Public Engagement and Planning Division.

A log of the following will be maintained by the ATIPP Coordinator for a minimum of 2 years after the Privacy Breach occurred:

- Date(s) of the breach.

- Date discovered.

- Who identified the breach (internally or externally) and their relationship to the Board.

- Who reported the breach to the C.E.O. of the Board, the Deputy C.E.O. and the Board's ATIPP Coordinator.

- Date reported to the C.E.O. of the Board, the Deputy C.E.O. and the Board's ATIPP Coordinator.

- Description of the incident.

- Cause of the breach.

- Number of individuals affected.

- Personal Information involved.

- Investigation process and representatives of the Board involved in the investigation.

- Steps taken to contain and mitigate the breach (short term).

- Corrective actions (long term).

- Disciplinary action if applicable (if breach was the result of employee fault or negligence).

- Who was notified of the breach externally.

- Dates of notification.

- Location of written communication with those affected, regulators, etc. (retain all communications).

- Date the case was closed

PROCEDURE: STEP 6 (TREND ANALYSIS AND PROCESS/POLICY REVIEW)

The ATIPP Coordinator will track and analyze all privacy breaches involving the Board, and determine if there are any trends with respect to that.

The C.E.O., in consultation with the ATIPP Coordinator and the Chairperson, will review the Board's policies and procedures concerning personal information and privacy breaches on an ongoing basis. Any necessary changes to the Board's policies and procedures will be made on an ongoing basis, as needed, in accordance with the applicable legislation.

SCHEDULE A

PRIVACY BREACH RESPONSE FORM

INSTRUCTIONS: To Be Completed by the ATIPP Coordinator

If you believe that there has been a breach of privacy regarding an employee or client, please immediately inform the C.E.O. of the Board, the Deputy C.E.O. and the Board's ATIPP Coordinator.

Please provide as much detail as possible.

Date Breach occurred	
Date Breach was discovered	
Person Identifying Breach	
Person Reporting Breach to ATIPP Coordinator	
Date Reported to ATIPP Coordinator	

1. Provide a detailed summary of the Breach (who, what, where, when?).

2. What was the cause of the Breach?

3. List the number and names of individuals affected by the Breach (if more space is needed, list the names on the back of the page).

4. What Personal Information was involved in this Breach (be specific)?

5. What Steps have you taken to investigate the Breach?

6. What Steps have you taken to mitigate the Breach (short-term)?

7. What suggestions do you have for corrective action (long-term) to ensure this Breach doesn't happen again?

8. Have any disciplinary or reinforcement of process or privacy awareness steps been taken (if Breach was a result of carelessness or error)?

9. Please provide other useful information regarding this Breach.

10. Who has been notified about the Breach? (External notification requires approval from the the Chairperson, in consultation with the C.E.O.). Provide the date of notification for approved external communication.

11. Date case closed.

IMPORTANT – Please ensure all written communication regarding this Breach is retained. It may be required as part of any investigation or follow up.