



WHISTLER

ADMINISTRATIVE PROCEDURE

PROCEDURE NUMBER: A-8

Privacy Breach

PURPOSE

This Privacy Breach Administrative Procedure (the “procedure”) defines a “privacy breach” and the “harm” that may result. The procedure describes the appropriate and immediate action to be taken by Resort Municipality of Whistler (RMOW) employees if a real or suspected privacy breach occurs. Gathering information regarding the nature and extent of the breach will optimize mitigation measures.

When a breach occurs that is suspected or known to compromise the physical safety of an individual or individuals, contact the RCMP in an emergency capacity.

SCOPE

This procedure applies to all RMOW employees, consultants and their employees, contractors and their employees, or any other person. All Users are expected to become familiar with and to comply with this procedure. Any RMOW employee who becomes aware of a possible breach of privacy involving personal information in the custody or control of the RMOW will immediately inform the Municipal Clerk.

All known or suspected privacy breaches require immediate remedial action regardless of the perceived sensitivity of the personal information. Actions to respond to the breach are proportional and appropriate to each breach.

All appropriate steps are taken with the pursuit of limiting the scope and effect of the breach. The Municipal Clerk and the Legislative and Privacy Coordinator will assist the department experiencing the breach with investigation into the cause of the breach as well as the steps to effectively mitigate any harm.

1 DEFINITIONS

“Privacy Breach”

is a collection, use, disclosure, access, disposal, or storage of personal information, whether accidental or deliberate, that is not authorized by the *Freedom of Information and Protection of Privacy Act (FOIPPA)*.

“Harm”

Can include, but is not limited to:

- a) Identity theft;
- b) Risk of physical harm;
- c) Hurt, humiliation, damage to reputation;
- d) Loss of business or employment opportunities;
- e) Breach of contractual obligations - Contract provisions may require notification to third parties in the case of a loss or privacy breach;
- f) Future breaches due to similar technical failures;
- g) Failure to meet professional standards or certification standards.

Harm to the public as result of the breach:

- a) Risk to public health;
- b) Risk to public safety.

Harm to the RMOW as result of the breach:

- a) Loss of trust;
- b) Loss of assets;
- c) Financial exposure;
- d) Legal exposure.

2 REPORTING A SUSPECTED OR CONFIRMED PRIVACY BREACH

2.1 Any RMOW employee who becomes aware of a possible breach of privacy involving personal information in the custody or control of the RMOW will immediately inform the Municipal Clerk. If the breach is suspected to be digital-related, the employee will also immediately inform the IT Department.

2.2 Reporting a suspected privacy breach to IT and the Municipal Clerk are strongly encouraged, even if uncertain that a breach has occurred; including but not limited to:

- a) Clicking on an unsafe link;
- b) Opening a corrupted file;
- c) Downloading a document from an unknown source.

3 ACTIONS TO LIMIT THE SCOPE AND EFFECT (HARM) OF THE BREACH

3.1 Limiting the scope

- 3.1.1 Isolate or suspend the activity that caused the privacy breach. This includes stopping the unauthorized practice, recovering the records, shutting down the system that was breached, or correcting weaknesses in physical security.
- 3.1.2 Take immediate steps to recover the personal information, records or equipment from all sources, where possible.

- 3.1.3 Determine if any copies have been made of the personal information in question and recover the copies where possible.
- 3.1.4 Where the privacy breach involves computer-based information, the direction of the IT Manager in conjunction with the Municipal Clerk must also be sought before taking any containment steps.

3.2 Personal Information Involved

- 3.1.1 Assess what data elements have been breached. Generally the more sensitive the data, the higher the risk.

3.2 Cause and Extent of the Breach

- 3.2.1 Identify the cause of the breach.
- 3.2.2 Identify if there is a risk of on-going or further exposure of the information.
- 3.2.3 Identify or estimate the extent of the unauthorized collection, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, including mass media and online.
- 3.2.4 Determine if the information is encrypted or not otherwise identifiable.
- 3.2.5 Assess the steps already taken to minimize the harm.

3.3 Individuals Affected by the Breach

- 3.3.1 Identify or estimate how many individuals are affected by the breach.
- 3.3.2 Identify the category of persons effected by the breach: e.g., employees, members of the public, Mayor and Council, contractors, customers, service providers, other individuals or organizations.

4 DOCUMENTING THE BREACH

4.1 To be carried out in parallel with mitigation actions until complete.

4.2 Document the privacy breach in detail, including:

- a) Events that led to the breach;
- b) Description of the breach;
- c) How and when the privacy breach was discovered;
- d) The personal information involved and the scope of the breach;
- e) Who was involved, if known;
- f) Individuals interviewed about the breach;
- g) Who has been notified;
- h) The corrective action taken, including any steps to assist affected individuals in mitigating harm, and;
- i) Recommendations, including corrective action that still needs to be taken.

5 NOTIFICATION

5.1 Determination of Notification:

- 5.1.1 The Municipal Clerk and Legislative and Privacy Coordinator will work with the department in question to determine if affected individuals should be notified and the timeframe of such notification.
- 5.1.2 The Manager of Finance will be notified due to contractual notification obligations of third parties in business with the RMOW.
- 5.1.3 In determining notification, the following information is required to be determined:
 - a) Existing contractual obligations that require notification;
 - b) A risk of identity theft or fraud;
 - c) A risk of physical harm (including stalking and harassment);
 - d) A risk of hurt, humiliation or damage to reputation.

5.2 When and How to Notify

- 5.2.1 Notification will occur as soon as possible following the breach. However, if law enforcement authorities have been contacted, those authorities will assist in determining whether notification will be delayed in order not to impede a criminal investigation.
- 5.2.2 The preferred method of notification is direct: by phone, letter, or in person – to affected individuals. Indirect notification: website information, posted notices, media will generally occur only where direct notification could cause further harm, is prohibitive in cost, or contact information is lacking.
- 5.2.3 Using multiple methods of notification in certain cases may be the most effective approach to ensure that the individual(s) are notified as quickly as possible.
- 5.2.4 The following is included in the notification:
 - a) Date of breach;
 - b) Description of breach;
 - c) Description of the information inappropriately accessed, collected, used or disclosed;
 - d) The steps taken to mitigate the harm;
 - e) Next steps planned and any long term plans to prevent future breaches;
 - f) Steps the individual can take to further mitigate the risk of harm;
 - g) Contact information for the Municipal Clerk and Legislative and Privacy Coordinator.
- 5.2.5 Other Contacts; notifying the following authorities or organizations should be considered by the Municipal Clerk, IT, Legislative and Privacy Coordinator, and department involved in the breach:
 - a) Police: if theft or crime is suspected;
 - b) Insurers: if required by contractual obligations;

- c) Third parties sharing network access with RMOW (e.g., banks, vendors, BC Transit, etc. – IT and all applicable departments will provide a complete list and assist with notification as required);
- d) Professional or other regulatory bodies: if professional or regulatory standards require notification of these bodies;
- e) Office of the Information and Privacy Commissioner (OIPC): The following factors are relevant in deciding when to report a breach to the OIPC:
 - The sensitivity of the personal information;
 - Whether the disclosed information could be used to commit identity theft;
 - Whether there is a reasonable chance of harm from the disclosure including non-pecuniary losses;
 - Whether the information was fully recovered without further disclosure.

6 REPORTING TO COUNCIL

6.1 The Municipal Clerk will assess when it is appropriate to inform and update Mayor and Council.


7 PREVENTION

7.1 Prevent privacy breaches by reviewing your departmental procedures. If applicable, implement any recommended changes or bring recommendations to the attention of Management/ Municipal Clerk.

Dated this 2 day of August, 2018.


Signed Original on File

Brooke Browning
Municipal Clerk


Signed Original on File

Mike Furey
Chief Administrative Officer