

PRIVACY BREACH MANAGEMENT POLICY TEMPLATE

June 2008

Policy Date: _____ <i>Most current policy review date</i>	Contact: <i>Contact information for individuals with questions about the policy and to identify the program area responsible for the policy</i>
---	--

Purpose: *State the purpose of the policy which will likely include:*

- *Obligation of all staff to report privacy breaches*
- *To describe process for managing privacy breaches*
- *To assign responsibilities and timelines*

Document Owner: *Program area and position responsible*

Policy Applies to: *Identify staff and/or contractors subject to policy*

Process Responsibility: *Likely the Privacy Officer or Director/Manager of Information Privacy*

Final Accountability: *Identify the management position responsible*

Policy Scope: *When does the policy apply?*

Definitions: *Include definitions of key words such as “personal information” and “privacy breach”.*

Action Plan/Steps in Managing a Privacy Breach:

Set out the steps in managing a privacy breach. Use the Office of the Information and Privacy Commissioner’s document, “Key Steps in Responding to Privacy Breaches” as a guide.¹ For each step, set out the action required, the individual responsible and the recommended time lines. Below are some recommended actions and suggested responsible positions and timelines.

¹ Available at: [http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches\(June2008\).pdf](http://www.oipc.bc.ca/pdfs/Policy/Key_Steps_Privacy_Breaches(June2008).pdf)

Action Required	Position Responsible	Recommended Timelines
1. Contain the breach.	Program area where breach occurred.	Immediate.
2. Report the breach within the organization or public body	<ul style="list-style-type: none"> • Program area staff (report to management) • Management (report to Privacy Officer or Director/Manager Information & Privacy (DMIP)) • PO & DMIP report to executive as required 	Same day as breach discovered
3. Designate lead investigator and select breach response team as appropriate	Privacy Officer or DMIP	Same day as breach discovered
4. Preserve the evidence	Lead Investigator, Privacy Officer or DMIP	Same day as breach discovered
5. Contact police if necessary	Privacy Officer or DMIP	Same day as breach discovered
6. Conduct preliminary analysis of risks and cause of breach	Lead Investigator	Within 2 days of breach discovery
7. Determine if the breach should be reported to the Privacy Commissioner	Privacy Officer or DMIP in consultation with executive	Generally within 2 days of breach
8. Take further containment steps if required based on preliminary assessment	Lead Investigator, Privacy Officer or DMIP	Within 2 days of breach
9. Evaluate risks associated with breach	Lead Investigator, Privacy Officer or DMIP	Within 1 week of breach
10. Determine if notification of affected individuals is required	Privacy Officer or DMIP	Within 1 week of breach
11. Conduct notification of affected individuals	Privacy Officer, DMIP or program area manager	Within 1 week of breach
12. Contact others as appropriate	Privacy Officer, DMIP or program area manager	As needed
13. Determine if further in-depth investigation is required	Privacy Officer, DMIP or program area manager	Within 2 to 3 weeks of the breach
14. Conduct further investigation into cause & extent of the breach if necessary	Privacy Officer, DMIP, security officer or outside independent auditor or investigator	Within 2 to 3 weeks of the breach
15. Review investigative findings and develop prevention strategies	Privacy Officer, DMIP or program area manager	Within 2 months of breach
16. Implement prevention strategies	Privacy Officer, DMIP or program area manager	Depends on the strategy
17. Monitor prevention strategies	Privacy Officer, DMIP or program area manager	Annual privacy/security audits

Roles and Responsibilities:

List the roles and responsibilities by position type.

Tools:

Develop and attach a breach reporting form for program areas.

Develop and attach checklists as appropriate for investigators.

Develop and attach a template breach notification letter that includes the following elements:

- Date of the breach
- Description of the breach
- Description of the information inappropriately accessed, collected, used or disclosed
- Risk(s) to the individual caused by the breach
- Steps taken so far to control or reduce the harm
- Future steps planned to prevent further privacy breaches
- Steps the individual can take to reduce the harm
- Privacy Commissioner contact information
- Organization contact information for further assistance

Related Policies

The public body or organization should have in place policies related to security of personal information including:

- General operational security standards
- Network access and security
- Data protection
- Security on portable storage devices
- Travelling with personal information
- Secure destruction of personal information