Privacy Breach Policy

1. About this document

This policy defines roles and responsibilities for the management of privacy breaches, whether suspected or confirmed. This policy identifies departments' responsibilities related to managing privacy breaches and requires departments to conduct investigations and deploy mitigation strategies.

2. Definitions

"Privacy Breach Reporting Form" means the form designed by the ATIPP office.

"Privacy Breaches", or personal information incidents, may include the accidental loss or alteration, as well as unauthorized access, collection, use, disclosure or disposal of either personal information or personal health information.

3. Application

This policy applies to all government departments as listed in GAM 2.1.

4. Authority

This policy is issued under GAM 2.27 and was approved by the Deputy Minister of HPW on October 20, 2016.

5. Roles and Responsibilities

Deputy Heads will:

- Ensure necessary resources (i.e. financial, technical, staff, etc.) are available to manage privacy breaches.
- Support their privacy officers in mitigating the risks of breaches and conducting investigations of suspected and actual breaches.
- Ensure the privacy breach protocol is followed by department staff.
- Approve departmental privacy breach procedures.
- Based on advice from the privacy officer, determine whether significant risks of harm exist following breach investigations.

Department staff will:

- Follow the government-wide privacy breach protocol.

- Use the approved privacy breach reporting form.
- Immediately report any suspected or actual privacy breaches to their supervisor or manager.

Program area managers will:

- Immediately report suspected or actual privacy breaches brought to their attention to their department's privacy officer.
- Cooperate with breach investigations being conducted by the privacy officer.
- Implement recommendations and mitigation strategies issued by their departmental privacy officer as a result of a privacy breach.

Privacy Officers, or a delegate, will:

- Ensure this policy is communicated to department staff.
- Develop any departmental privacy breach procedures in accordance with GAM 2.27 and submit for review to the Deputy Minister.
- Review completed privacy breach reporting forms and inform Deputy Minister of risks of significant harm.
- Investigate reported breaches and suspected breaches with assistance from program area managers.
- Provide recommendations and mitigation strategies, incorporating input from program area managers and the ATIPP office as needed.
- Submit completed privacy breach reporting forms, within a reasonable amount of time following an investigation, to the director of Corporate Information Management, if the Deputy Minister determines there is a risk of significant harm.
- Report annually to the director of Corporate Information Management, including the number of reported privacy breaches, the number of individuals affected, and the number deemed to have a risk of significant harm.

The ATIPP Office will:

- Maintain and update forms, templates and guidance documents.
- Assist privacy officers and program area managers with investigating and developing mitigation strategies as a result of privacy breach, when requested;
- Review and comment on completed privacy breach reporting forms, when requested.
- Track and report on privacy breaches where it is determined by departments there exists a risk of significant harm.