GOVERNMENT OF YUKON POLICY 2.27

GENERAL ADMINISTATION MANUAL

VOLUME 2: HIGHWAYS AND PUBLIC WORKS POLICIES

TITLE: PRIVACY MANAGEMENT POLICY

EFFECTIVE: October 27, 2015

---

1 SCOPE

1(1) Authority

(a) This directive is issued under the authority of the Deputy Ministers' Review Committee meeting #15-11 dated October 27, 2015. Authority for managing personal information in the custody or control of Government of Yukon (YG) is established by the *Access to Information and Protection of Privacy Act* (ATIPP Act) and, for personal health information by the *Health Information Privacy and Management Act* (HIPMA).

1(2) Application

(a) This directive applies to all government departments as listed in GAM 2.1.

1(3) Purpose

(a) The purpose of this policy is to apply authorities and responsibilities to YG departments in the management and protection of personal information, referred to as Privacy Management (PM). Privacy management is essential for protecting Yukoners' personal information, including personal health information, as required under the ATIPP Act and HIPMA; since the public is required to share personal information with the government in order receive services, YG is held to a high standard of privacy protection.

1(4) Definition

(a) **Personal information** is as defined in the ATIPP Act.

(b) **Personal information incident** means access, collection, use, disclosure, retention or disposal of data that is not authorized under applicable law. An incident may occur as a result of inadvertent error or malicious action by employees, third parties, or intruders.

(c) **Privacy** is an individual's right to have their personal information protected from unauthorized collection, use and disclosure.

(d) **Privacy Advisory Committee** refers to a committee of privacy officers established to share information and lessons learned; it is chaired by Director of Corporate Information Management.

(e) **Privacy Impact Assessments** are a standard tool used to identify and mitigate potential privacy risks of new or redesigned government IT systems, programs, services or legislation, based on a standard template provided by HPW.

(f) **Privacy Management Program** means the overarching program put in place by Highways and Public Works to which departments must adhere.

(g) **Privacy Management Plans** are implemented at the department or program level based on a standard template provided by HPW, and are the mechanism by which departments fulfill their responsibilities under the privacy management program, such as collection, use, disclosure and retention, as well as incident management.

2 PRIVACY MANAGEMENT PROGRAM

2(1) Privacy management authority and leadership

(a) In accordance with section 3 of this document: on roles and responsibilities, and subsequent GAM policies, Highways and Public Works provides leadership, issues guidance documents, standards, training materials and supporting policies to assist departments to deliver and adhere to corporate information privacy policies.

(b) Highways and Public Works hosts the Corporate Information Management (CIM) office, which ensures there is corporate guidance on the ATIPP Act.

(c) Health and Social Services is responsible for developing regulations and standards for personal health information (PHI) under HIPMA. All departments designated as custodians under the Act must follow the standards required by HIPMA. Where the privacy program requirements exceed HIPMA's standards, the privacy program's requirements will need to be applied in addition to HIPMA.

2(2) Privacy Management Program Elements

(a) The personal information map is a complete accounting of the categories, amount, sensitivity and location of personal information within the custody and control of YG program areas, along with the purpose for which it is collected, used and disclosed; it does not contain any personal information itself. This map allows Highways and Public Works to assess what kinds of information are held by government and in which departments, how information flows through the administrative network, and whether these information holdings comply with privacy management best practices, as well as the ATIPP Act. The personal

information map enhances risk management and provides a mechanism for the public to know which departments hold what kinds of information.

(b) Privacy management policies and procedures lay out essential, standardized requirements for protecting personal information in each of the following areas, primarily through completion of a Privacy Management Plan in individual program areas:

  (i) Collection, use and disclosure of personal information;

  (ii) Retention and disposal of personal information, once the information is no longer required for business or legal purposes;

  (iii) Security of personal information, as per the Information Security GAM;

  (iv) Handling complaints related to the public body's management of personal information, and other areas deemed necessary for privacy management.

(c) Contractor management controls ensure that non-government organizations, and individuals acting on behalf of YG, collect, use, disclose and dispose of information in a manner that protects Yukoners' personal information to the standard set by the privacy management program. These controls emphasize the public body's ultimate responsibility for protecting information to a high standard even if another organization is acting on behalf of the public body.

(d) Standard risk assessment and mitigation processes are used, including privacy impact assessments (PIAs), for personal information collected, used or disposed of by government. PIAs, along with other risk management tools, help prevent personal information incidents.

(e) Incident management processes mitigate personal information incidents, or breaches, which occur when personal information has not been handled in accordance with legislation, collection, use, disclosure, retention and disposal policies, and security safeguards. By following a consistent process for managing incidents, the impact of an incident can be limited and lessons learned can be applied in other areas to prevent a similar breach from occurring in the future. This is achieved primarily by updating a privacy management plan in individual program areas.

(f) Effective oversight that ensures compliance with the privacy management program supports departments in fulfilling their responsibilities under the ATIPP Act and HIPMA.

(g) Reporting is used to assess compliance, influence best practices, share lessons learned between departments, and communicate with the public. Individuals and organizations that are impacted by YG collection, use, disclosure, retention or disposal of personal information are able to access information about the privacy management program, its objectives, practices, policies, reporting and compliance

except where withholding that information is justified under a legislative provision.

(h) Training is provided to employees to increase their awareness of privacy protection, and ensure that they understand their responsibilities for handling personal information within their public service role.

3 ROLES AND RESPONSIBILITIES

3(1) The Deputy Ministers Review Committee (DMRC) is responsible for:

(a) Approving the GAM policy, including roles and responsibilities, related to privacy management.

3(2) Deputy Ministers are responsible for:

(a) Ensuring that privacy protection is a priority within their respective departments, and that departments have adopted privacy management practices and implemented government-wide policies within their program areas.

(b) Ensuring employees are trained in privacy management and protection principles.

(c) Ensuring contractors delivering a service or program for the department comply with the privacy management plan.

(d) Appointing privacy officers.

(e) Establishing responsibilities for privacy within their departments.

(f) Approving PIAs and privacy management plans prepared within their departments, or delegating this responsibility to a designate.

3(3) Highways and Public Works is responsible for:

(a) Developing and delivering the privacy management program, through the CIM office, across YG.

(b) Providing direction to departments and advising on requirements under the ATIPP Act.

(c) Supporting the development and resourcing of staff training to support a privacy-aware corporate culture.

(d) Developing and distributing privacy management policy guidance, templates and standards to department privacy officers to ensure a consistent approach.

(e) Working collaboratively with department staff to develop PIAs and privacy management plans, reviewing proposed final versions and providing written recommendations, if required, to the Deputy Minister prior to approval.

(f) Reviewing departments' incident management processes and ensuring they are implemented.

(g) Acting as the corporate point of contact and ongoing liaison with the Information and Privacy Commissioner.

(h) Ensuring departments comply with the privacy management program, auditing privacy management plans, and reporting on progress.

(i) Making information about the privacy management program available to the public.

(j) Chairing the Privacy Advisory Committee.

3(4) Privacy officers are responsible for:

(a) Working with program areas to develop and implement privacy management plans that include risk assessments, as per the PIA operational policy.

(b) Providing draft and complete PIAs to the CIM office within Highways and Public Works.

(c) Overseeing submitting information for the personal information map to Highways and Public Works for approval.

(d) Ensuring that information incidents are reported to Highways and Public Works.

(e) Ensuring that reporting and audit requirements set by Highways and Public Works are met.

(f) Participating in the Privacy Advisory Committee.

3(5) Employees are responsible for:

(a) Complying with the privacy management program, and the privacy management plan in place within their department or program area.

(b) Increasing their awareness of privacy requirements and best practices.

(c) Committing to training on privacy protection, as required.