Privacy Analyst

DEFINITION

This is a professional, semi-independent, level of work related to the assessment and response to privacy impact. The work involves the application of knowledge acquired through specific education and work experience.

The Privacy Analyst classification plays a key directive and consultative role with other areas of the City developing privacy impact assessments (PIAs); PIAs are used to identify, assess, and manage risks associated with personal information that is collected, used, or disclosed as a result of implementing a new initiative or as a result of changing an existing initiative.

This classification is responsible for supporting the City's Privacy Protection program. This classification ensures programs and services are designed in compliance with privacy legislation and principles.

This classification is responsible for assessing privacy risks and identifying safeguards for a variety of systems including those related to analytics, open data, privacy ethics, big data, business intelligence, and machine learning. This position is delegated on behalf of the City Manager to make significant decisions with respect to the protection of privacy in accordance with the *Freedom of Information and Protection of Privacy* (FOIP) *Act*.

This classification provides advice to business areas regarding privacy risk assessment and semi-independently makes decisions and supports the Privacy Unit. Decisions falling outside typical processes and procedures and issues that are potentially politically sensitive or contentious in nature are escalated to the Corporate Privacy Advisors. There is not an automatic progression between this classification and the Corporate Privacy Advisor classification.

TYPICAL DUTIES *

Determines when a PIA is necessary on proposed initiatives; reviewing proposals and assigning a level of risk.

Guides operational areas through the assessment process, ensuring that business areas fully complete the PIA documentation.

Facilitates and leads multi-disciplinary teams to provide advice on privacy proposals, refine business processes, and determine the completeness of a PIA.

Privacy Analyst

Determines how to notify individuals about the collection of personal information and responding to inquiries from the public regarding the City's collection, use, disclosure, retention, and destruction of personal information.

Advises on draft contracts and agreements regarding ethical and legislative requirements to protect privacy.

Develops forms and templates for all City staff to ensure the protection of privacy in accordance with ethical and legislative requirements.

Resolves concerns from individuals who have been affected by a privacy breach or privacy complaints and who have been notified of the breach by the City.

Assists in following up on recommendations from privacy breach investigations, ensuring compliance with recommendations.

Provides training to staff on privacy matters, including training when it is a recommendation following a privacy breach incident.

Processes access to information requests in accordance with the FOIP Act and the City's FOIP Delegation Order, when required.

KNOWLEDGE, ABILITIES AND SKILLS

Demonstrated experience performing, reviewing, and facilitating privacy impact assessments.

Demonstrated experience developing and applying policies and procedures.

Demonstrated experience designing and delivering access and privacy training.

Demonstrated research, analysis, synthesis and problem solving skills to gather required information, make decisions and develop recommendations.

Demonstrated knowledge of records management principles.

Demonstrated written and verbal communication skills.

Demonstrated experience in the development and writing of reports and briefings.

Demonstrated ability to work independently and as appropriate make decisions on issues that may be sensitive, time sensitive and or confidential.

Demonstrated skill in exercising good tact, sound judgement and firmness in dealing with difficult situations.

Privacy Analyst

Demonstrated ability to meet deadlines, and handle situations requiring diplomacy and tact.

Demonstrated ability to critically analyze issues to make decisions, recommend viable and effective solutions and summarize and manage information.

Demonstrated ability to handle and manage sensitive and confidential information.

Demonstrated ability to commit a high degree of attention to detail.

Demonstrated ability to utilize software for the completion of reports and records.

Demonstrated consulting and conflict resolution skills including ability to handle and address controversial situations, including experience with mediation.

TRAINING AND EXPERIENCE REQUIREMENTS

Job Level

University Degree in Information Studies, Public Policy, Archives Studies, Library Studies, Political Studies or a relevant discipline is required.

Information Access and Protection of Privacy (IAPP) certificate or equivalent from the University of Alberta, a recognized post secondary institution or a recognized professional association is required.

Minimum of four (4) years of directly related, progressively responsible experience working in the research, analysis, interpretation and application of access and privacy legislation is required.

*   *This is a class specification and not an individualized job description. A class specification represents and defines the general character, scope of duties and responsibilities of all positions within a specific job classification. It is not intended to describe nor does it necessarily list the essential job functions for a specific position in a classification. Positions may perform some of the duties listed above but this does not necessarily qualify for placement into this classification.*