



Classification:	Band 3	Position:	00146299
Reports to:	Director of Emerging Technologies	Location:	Victoria

Context

The OIPC provides independent oversight and enforcement of BC’s access and privacy laws under the *Freedom of Information and Protection of Privacy Act* (FIPPA) and the *Personal Information Protection Act* (PIPA). The newly established Emerging Information and Privacy Technologies team advances the Office’s regulatory framework, workflows, and understanding of emerging technology so that the office can quickly respond to projects, legislation, and complaints about emerging information and privacy technologies (e.g. automated decision-making tools, surveillance technologies, biometrics).

The Senior Investigator, Emerging Technologies leads technical investigations and audits with considerable independence, based on their extensive knowledge of technology audit and review practices. The position researches and evaluates architectural designs, security controls, and risk management practices to identify their existing and potential effects on data access, security and privacy. The Senior Investigator, Emerging Technologies will also work closely with policy and legal experts to draft clear and concise deliverables (e.g. briefing notes and high-profile public reports) and assess artificial intelligence systems and governance processes. Beyond these core activities, the Senior Investigator, Emerging Technologies provides expert technical advice and guidance within the OIPC, including to Investigators, Auditors, and Case Review Officers who handle complex files related to data breaches.

Accountabilities

- Leads technical investigations, audits, and reviews which may include preparing and conducting technical assessments, risk analyses, security controls reviews, and other technical reporting.
- Reviews and evaluates the technological aspects of proposed public sector information systems, programs, and initiatives, which may include assessing architectural diagrams, data schemas, and software code.
- Provides authoritative technical investigative advice on investigations, audits, privacy impact assessments, algorithmic assessments, privacy management programs, common and integrated program agreements, connected services agreements, and special projects involving digital technologies, as needed.
- Develops project proposals and plans (e.g. scope, criteria, tools, resources, risks and timelines), briefing notes, reports for publication, and other communications regarding audits, investigations, and reviews.

- Conducts research and analysis on information technologies to better position executive leadership with an understanding of how those technologies relate to access and privacy rights.
- Identifies training requirements for the office and develops and delivers technical guidance or educational materials for OIPC staff, external parties and British Columbians on de-identification, privacy enhancing technologies, surveillance technologies, artificial intelligence technologies, and/or data access issues.
- Provides advice to senior leadership in the development of technical investigation and review procedures, formulates and recommends improvements to service delivery for requests for review and complaints, and supports senior leadership in aligning operations with the achievement of the office's strategic goals.
- Liaises with public authorities and private organizations, provides authoritative technical information, guidance, and recommendations for legislative compliance; monitors implementation of recommendations, and works with officials to address privacy and access issues.
- Maintains contacts and links with external stakeholders, including but not limited to: government agencies (senior FOI and privacy officials in ministries, crown corporations, boards, commissions and agencies, school districts and educational institutions, local governments, and other public bodies); private organizations (corporations, trade unions, trusts, not-for-profit organizations, and unincorporated associations); and the general public.
- Peer reviews the work of Investigators and is available to the Director of Case Review and Case Review Officers to provide expert guidance regarding access and privacy matters.
- Represents the office on national and international projects, committees and conferences when called upon by a senior staff member to do so.
- Procures and supervises contractors, consultants, or cooperative students to support investigations and research.

Qualifications

Education and Experience:

- University Degree in a related field (e.g. Computer Science, Computer Engineering, Data Science, Information Studies, Cybersecurity, Public Policy, Public Administration, Indigenous Business and Public Administration, Political Science, Information Law, Joint Juris Doctor/Indigenous Law).
- Three years of experience conducting technical audits, research, or investigations, which includes experience collecting and assessing technical evidence, and formulating recommendations or findings based on that evidence.
- Three years of work involving implementation of, or familiarity with, the *Freedom of Information and Protection of Privacy Act* (FIPPA) and/or the *Personal Information Protection Act* (PIPA) and/or evaluating compliance with FIPPA, PIPA or similar regulatory statute.
- Proven expertise in technology design or assessments, with strong knowledge of issues related to auditing AI, cybersecurity, data governance, quantum computing, surveillance technologies or digital transformation.
- Experience supervising or mentoring employees.
- Experience working with a broad cross-section of the public sector and private sector.
- Successful completion of security screening requirements of the BC Public Service, which may include a criminal records check (completed if an offer of employment is made).

- An equivalent combination of education and experience, such as extensive (4 or more years) hands-on experience with technical audits or investigations, may be considered.

Preference may be given to applicants with the following:

- Professional designation in a related field (e.g. CIPT, CISA, CISSP, ISO:27001 Lead Auditor, or similar).
- Experience or formal education in auditing AI and automated decision-making systems.

Proviso:

- Demonstrated commitment to anti-racism, respect, and inclusivity.
- Remains current on FIPPA, PIPA and emerging information and privacy protection legislation, regulations and policies within British Columbia, and in other jurisdictions.

Knowledge, Skills and Abilities:

- Familiarity with access and privacy laws and principles, FIPPA, PIPA, and the mandate of the Information and Privacy Commissioner, or a similar regulatory body and its statutes.
- Comprehensive knowledge of the benefits and privacy or freedom of information challenges related to evolving technologies such as genomics, agentic AI, quantum computing, complex surveillance systems, and digital health tools.
- Understanding of the risks, ethical and fairness considerations associated with AI in public service delivery.
- Knowledge of the latest trends, developments, issues, legal decisions and precedents relating to digital technology, access to information and protection of privacy.
- Strong investigative skills including the ability to prepare investigative plans, gather evidence, establish fact patterns, and identify relevant policies and procedures.
- Effective written and oral communication skills and the ability to communicate complex ideas clearly and concisely in written reports, correspondence, and discussions with the public and senior officials.
- Proven ability to work independently with little oversight and produce high-quality work while managing a diverse and demanding workload.
- Proven ability to work effectively as part of a team and to develop effective working relationships with executive, colleagues, and contacts in the private and public sector.
- Ability to use a variety of computer programs including word processing, managing spreadsheets for large data sets, and performing simple statistical and analytical methods.
- Ability to lead, advise and provide feedback to staff to effectively manage large investigations and achieve business goals and objectives.
- Demonstrated ability to maintain objectivity and deliver a high quality of service under sometimes stressful conditions.
- Ability to act proactively as well as to use tact, discretion and sound judgement.
- Knowledge of the rules of natural justice and administrative fairness.

Competencies:

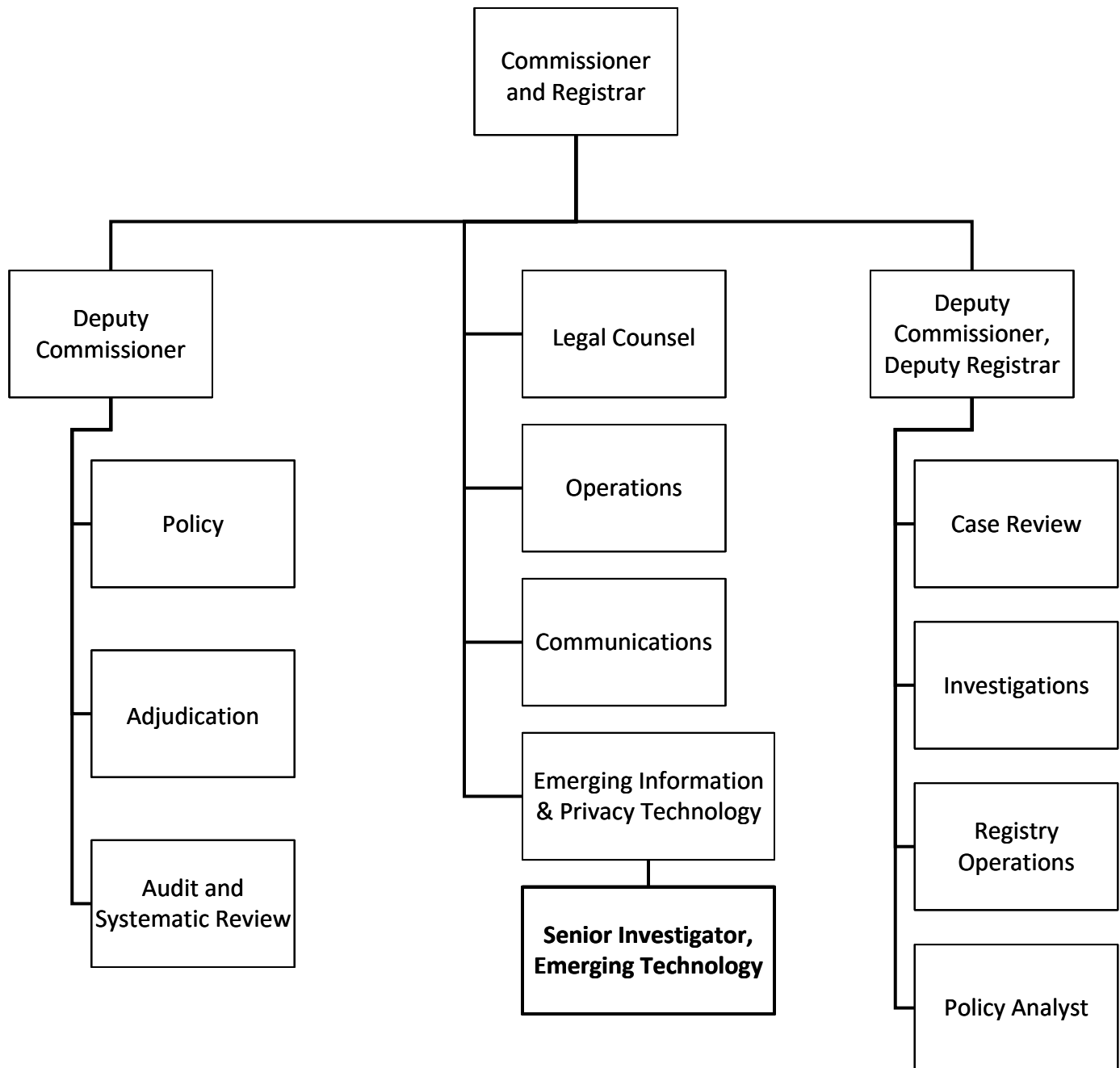
- **Change Management** is the ability to support a change initiative that has been mandated within the organization. It involves helping the organization's members understand what the change means to them and providing the ongoing guidance and support that will maintain enthusiasm and commitment to the change process. People with this competency willingly embrace and champion change. They take advantage of every opportunity to explain their vision of the future to others and gain their buy-in.
- **Results Orientation** is a concern for surpassing a standard of excellence. The standard may be one's own past performance (striving for improvement); an objective measure (achievement orientation); challenging goals that one has set; or even improving or surpassing what has already been done (continuous improvement).
- **Conceptual Thinking** is the ability to identify patterns or connections between situations that are not obviously related, and to identify key or underlying issues in complex situations. It includes using creative, conceptual or inductive reasoning or thought processes that are not necessarily categorized by linear thinking.
- **Engaging External Partners** identifies and involves external stakeholders to foster long term partnerships.
- **Teamwork and Co-operation** is the ability to work co-operatively within diverse teams, work groups and across the organization to achieve group and organizational goals. It includes the desire and ability to understand and respond effectively to other people from diverse backgrounds with diverse views.
- **Organizational Commitment** is the ability and willingness to align one's own behaviour with the needs, priorities, and goals of the organization, and to promote organizational goals to meet organizational needs.
- **Leadership** implies a desire to lead others, including diverse teams. Leadership is generally, but not always, demonstrated from a position of formal authority. The "team" here should be understood broadly as any group with which the person interacts regularly.
- **Self-Discovery and Awareness** means understanding one's thoughts, feelings, values and background and how they impact the success of the interaction and relationship, or how they may influence one's work. It is recognizing one's own biases by tracing them to their origins, through reflection and by noticing one's own behaviour—and then intentionally seeking a way forward that positively impacts the interaction and relationship. It means maintaining new ways of thinking and acting when situations become difficult or uncertain, or in times of urgency.

BC's Information and Privacy Commissioner

Promoting and protecting the information and privacy rights of British Columbians.

<http://www.oipc.bc.ca/>

Office of the Information and Privacy Commissioner



Note:

- This is a high-level org-chart for recruitment purposes only.
- The structure is effective January 2026 and is subject to change.
- This document may not be compatible with screen readers. Please contact us if you have questions about the organizational structure.