

## Update

Ministry

**Describe: Basic Job Details****Position**

Position ID

Position Name (30 characters)

Current Class

Job Focus

Supervisory Level

Agency (ministry) code

Cost Centre

Program Code: (enter if required)

**Employee**

Employee Name (or Vacant)

**Organizational Structure**

Division, Branch/Unit

 

Supervisor's Position ID

Supervisor's Position Name (30 characters)

Supervisor's Current Class

**Design: Identify Job Duties and Value****Changes Since Last Reviewed**

Date yyyy-mm-dd

Responsibilities Added:

Responsibilities Removed:

**Job Purpose and Organizational Context**

Why the job exists:

security requirements of the Health Information Act (HIA), the Freedom of Information and Protection of Privacy Act (FOIP), and adherence to the Department's Information and Security Management Directives.

Central to the position is overseeing the development and maintenance of the Privacy Impact Assessment process for the department and Security Assessments processes ensuring Alberta Health activities are security and privacy enhancing where possible; and monitoring departmental compliance with the privacy provisions of *HIA* and *FOIP*. This position provides health information privacy and security expertise as required to support Information Management initiatives.

This position is also responsible for working with multiple health sector stakeholders for managing security of the Electronic Health Record.

This position works closely with the *Health Information Act* (HIA) Policy Unit to ensure the requirements of the HIA and other pertinent legislation are appropriately managed. The position provides policy input and expertise with respect to security and privacy issues. The position works with both internal stakeholders within the Department and external stakeholders across the health sector. This requires working closely with the Technology and Innovation's Cybersecurity Division to manage GOA security; and developing and recommending departmental security strategies and processes to senior management.

## Responsibilities

Job outcomes (4-6 core results), and for each outcome, 4-6 corresponding activities:

Development and maintenance of the department's Privacy Impact Assessment and Security Assessment advice and processes:

- Maintain and operate privacy and security intake processes;
- Lead team in development of privacy impact assessments where required;
- Lead team in development of security assessments where required;
- Identification and completion of privacy and security risk identification, advice, and necessary governance obligations including vulnerability, penetration testing, security assessments for department and partner/stakeholder initiatives; and,
- Maintain privacy impact assessment and security assessment processes.

• Providing subject matter expertise and advice from a privacy and security perspective to support department initiatives:

- Existing and new cross-ministry and provincial initiatives including Alberta Netcare and eHealth initiatives; and,
- Data governance/access.

• Provide advice and recommendations on the development, maintenance and implementation of Alberta Health's Information Management Security Directives.

- Inform cybersecurity policy development and implementation for the department; and,
- Advice provision across various teams supporting compliance with information security management directives.

• Provide advice and recommendations on the mitigation of privacy and security issues as they pertain to the provincial EHR, eHealth and internal departmental systems and processes.

- Provide analyses, options and recommendations on technical and process related issues both as requested by the stakeholders and on a proactive basis. The analysis includes review of acts, regulations, policies, procedures and industry best practices.
- Provide stakeholders with timely responses that allow for practical implementation of the security controls required to effectively mitigate risk, while not unduly delaying the implementation of the EHR or other departmental systems.
- Monitoring and guiding operational EHR privacy and security deployment concerns includes security assessments (pORA), ensuring alignment to PIAs, EHR access role review.

• Provide advice and direction on incident management processes:

- Ensure the Provincially Reportable Incident Response Process is maintained, applied and managed as required and issues mitigated

appropriately;

- Provide advice and guidance to Information Technology Operations and other programs on incident management; and,
- Monitoring and guiding security investigations, collaborative operation of provincial incident response and resolution activities.

## Problem Solving

Typical problems solved:

- Strong problem solving skills to resolve issues, balance competing interests, identifying risks and compliance issues .
- Logic and analytical skillset to identify and apply legislation or privacy and security policies (e.g. knowledge of health specific privacy, security, and access legislation (HIA and FOIP acts) and principles.)
- Interpersonal skills working with the department and other health related organizations as well as other department contacts at various levels.
- Balances competing interests and prioritizes a complex and heavy workload.
- Fast learner, effective verbal and written communicator.
- Maintain awareness of existing and emerging information security and privacy issues and trends, and their implications to program areas.

Types of guidance available for problem solving:

- Preparation of advice following background, analysis, and recommendation format.
- Development of team expertise and knowledge through formal training and self-supported learning plans.
- Identification and publishing of reusable advice and business-focused self-service support materials.

Direct or indirect impacts of decisions:

- Timely and accurate advice is critical to enabling initiatives to succeed while balancing privacy and security risks.
- Advice must consider risks associated with cyber-security incidents and privacy breaches impacting individuals and department reputation.

## Key Relationships

Major stakeholders and purpose of interactions:

### Internal

*Director, HSCPO:* Close liaison with the Director to provide privacy and security advice and to ensure coordination of issues and efforts. Weekly frequency.

*IMIT Project Program Managers and IT Operations:* Conducting privacy impact assessments, security assessments and provisioning advice. Daily frequency.

*Managers:* Consulting on privacy and security matters and investigations. Weekly frequency

*Privacy and Security Staff:* Providing advice and training, guidance, and mentorship. Daily frequency

*Executive Directors:* Provide advice and status on assessment activities and privacy/security risk management. Monthly frequency.

### External

*Office of the Information and Privacy Commissioner:* Consulting on privacy matters, privacy impact assessments, investigations or security matters. Weekly frequency.

*Stakeholders in Alberta's Health Sector (Alberta Health Services, Covenant Health, Colleges of Regulated Health Professions):* Providing privacy or security advice, gaining feedback on AHW privacy initiatives. Weekly frequency.

*GoA Cyber Security and Privacy Divisions:* Participating in GoA privacy or security initiatives and providing AH perspective. Monthly frequency

*Other GOA Departments:* Participating in GoA initiatives and providing AH perspective and supporting senior officials. Monthly frequency

*Albertans:* Answering inquiries and investigating complaints. As required.

## Required Education, Experience and Technical Competencies

Education Level <b>Bachelor's Degree (4 year)</b>	Focus/Major <b>Other</b>	2nd Major/Minor if applicable	Designation
--	-----------------------------	-------------------------------	-------------

If other, specify:

**Information Systems Security Management, Information Technology, Information Systems, Public Administr**

Job-specific experience, technical competencies, certification and/or training:

- Related university degree, post-secondary certificate or diploma (or equivalences);
- Certificate in Information Access and Protection of Privacy (IAPP) or 5 years equivalent real-world experience;
- Certified Information Systems Security Professional (CISSP) or 5 years equivalent real-world experience;
- Experienced leading and maintaining teams with broad organizational roles, responsibility and skillsets;
- Ability for self and teams to work independently, collaboratively, cooperatively, and productively with other individuals and teams within and external to the department;
- Strong verbal and written communication skills, including necessary briefing up, documentation, and presenting to senior leadership
- Strong analytical, problem identification, and organizational/tracking or project management skills;
- Strong relationship building skills, seek to understand problems and to propose solutions (consensus or otherwise);
- Knowledge and/or experience with the health system desirable.

## Behavioral Competencies

Pick 4-5 representative behavioral competencies and their level.

Competency	Level					Level Definition	Examples of how this level best represents the job
	A	B	C	D	E		
<b>Systems Thinking</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<b>Integrates broader context into planning:</b> <ul style="list-style-type: none"> <li>• Plans for how current situation is affected by broader trends</li> <li>• Integrates issues, political environment and risks when considering possible actions</li> <li>• Supports organization vision and goals through strategy</li> <li>• Addresses behaviours that challenge progress</li> </ul>	
<b>Creative Problem Solving</b>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<b>Works in open teams to share ideas and process issues:</b> <ul style="list-style-type: none"> <li>• Uses wide range of techniques to break down problems</li> <li>• Allows others to think creatively and voice ideas</li> <li>• Brings the right people together to solve issues</li> <li>• Identifies new solutions for the organization</li> </ul>	

Drive for Results	<input type="radio"/> <input type="radio"/> <input type="radio"/> <input checked="" type="radio"/> <input type="radio"/>	Works to remove barriers to outcomes, sticking to principles: <ul style="list-style-type: none"> <li>• Forecasts and proactively addresses project challenges</li> <li>• Removes barriers to collaboration and achievement of outcomes</li> <li>• Upholds principles and confronts problems directly</li> <li>• Considers complex factors and aligns solutions with broader organization mission</li> </ul>	
-------------------	--	---	--

**Benchmarks**

List 1-2 potential comparable Government of Alberta: [Benchmark](#)

Manager, Security Management and Operations (M410-05)
Manager, Health System Architecture (M410-31)

**Assign**

The signatures below indicate that all parties have read and agree that the job description accurately reflects the work assigned and required in the organization.

_____ Employee Name	_____ Date yyyy-mm-dd	_____ Employee Signature
_____ Supervisor / Manager Name	_____ Date yyyy-mm-dd	_____ Supervisor / Manager Signature
_____ Director / Executive Director Name	_____ Date yyyy-mm-dd	_____ Director / Executive Director Signature