Update

Ministry

Health

Describe: Basic Job Details

Position

Position ID

Position Name (30 characters)

Senior Security Analyst

Current Class

Systems Analyst Level 3

Job Focus

Operations/Program

Supervisory Level

00 - No Supervision

Agency (ministry) code

Cost Centre

Program Code: (enter if required)

Employee

Employee Name (or Vacant)

Vacant

Organizational Structure

Division, Branch/Unit

SPP/DAIP/HSCPO

☐ Current organizational chart attached?

Supervisor's Position ID

Supervisor's Position Name (30 characters)

Manager Privacy and Security

Supervisor's Current Class

Manager (Zone 2)

Design: Identify Job Duties and Value

Changes Since Last Reviewed

Date yyyy-mm-dd

2025-02-20

Responsibilities Added:

-Edits to reflect current organization structure and positions.
-Edits to reflect current security practices and processes.
-Added references to NIST frameworks.

Responsibilities Removed:

-Removed previous organization structure and positions.
-Removed outdated security processes and practices.

Job Purpose and Organizational Context

Why the job exists:

Reporting to the Manager, Privacy and Security, the Senior Security Analyst role requires the ability to react to dynamic, high-priority situations and guide stakeholders towards timely remediation. This includes managing the response to provincial health sector security incidents that have a significant impact to the confidentiality, integrity or availability of health systems. The role involves coordinating stakeholders, facilitating rapid decisions and actions,

and escalating issues as needed.

Proactivity in addressing health sector issues through research and analysis is essential. The position requires a mix of technical and soft skills to handle multiple competing issues simultaneously, such as incidents affecting patient data integrity, policy guidance for new projects, and threat and risk assessments. The Senior Security Analyst anticipates sophisticated attacks on health information, identifies system gaps, and creates solutions to close them. The role requires an ability to manage competing priorities appropriately.

Responsibilities

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

The Senior Security Analyst works closely with the Manager, Privacy and Security to maintain Information Security for both the department and the provincial health sector. Overall, Information Security Officers are tasked with protecting the Government of Alberta (GoA)'s information assets from a confidentiality, integrity, and availability perspective. They identify, assess, monitor, detect, investigate, research, and respond to threats and incidents impacting the security of information assets.

Key Responsibilities:

- **Information Security Maintenance and Monitoring**:
    - Develop, implement, maintain, and monitor the department's information security program, including policies, standards, practices, and processes.
    - Ensure provincial information security policies and standards are adhered to for all custodians connecting to the Electronic Health Record (EHR).
    - Monitor information security compliance in the department and the health sector through testing and ensuring appropriate remediation.
    - Support the maintenance and communication of expertise through a multi-faceted information security awareness program.
    - Respond to queries from business areas on exceptions and unique scenarios to provide flexibility while managing security appropriately.
- **Project Management and Collaboration**:
    - Lead and manage projects for information security initiatives, ensuring project deliverables are completed within time and budget.
    - Work collaboratively with IT project teams to vet project deliverables, complete security threat risk assessments, and assist project teams in making informed decisions.
    - Work with information owners or controllers to complete security testing and communicate results and mitigation approaches.
    - Participate in projects as an information security subject matter expert.
    - Mentor and coach junior staff and lead or coordinate small projects or activities.
- **Security Reviews and Incident Management**:
    - Facilitate, supervise, and coordinate information security reviews, including Vulnerability Assessments, Penetration Testing, and assisting external audit reviews.
    - Document, manage, and resolve provincial incidents, and report to Senior Management and others as required.
    - Lead the departmental information security incident response process and manage critical or escalated incident responses.
    - Monitor incident tickets and participate in on-call incident support rotation.
    - Complete Information Security Incident reports and provide updates regarding incident response

and resolution to management.

- **Threat Intelligence and Risk Management**:
    - Identify, assess, and treat information and technology security threats and risks.
    - Document risks in the GoA's Information Technology Security Risk Register.
    - Communicate cyber threat information to stakeholders and perform related research.
    - Analyze threat and risk information to formulate recommendations for improving security posture.
    - Maintain awareness of current threats and provide regular executive reporting on security posture, current threats, incidents, and measures.
- **Technical Security Controls and Disaster Recovery**:
    - Maintain knowledge of current threats and configure security equipment to mitigate these threats.
    - Recommend controls to ensure a tight security posture while enabling business requirements.
    - Enhance security systems management skills through research, peer support, and training.
    - Participate in the development of awareness or training material and facilitate in-class sessions.
    - Recommend considerations and assist program areas in completing documents and supporting enterprise IMT Disaster Recovery.

This position requires excellent interpersonal skills to work with both technical and non-technical staff within the unit, the Department, the government, the public, and various health sector organizations to support the implementation of security controls and legislation.

Problem Solving

Typical problems solved:

The Senior Security Analyst is responsible for providing subject matter expertise on the implementation of security controls within the Provincial Health System. This position involves identifying required reviews, analysis, and subsequent quality assurance for health systems and security controls assessment.

Nature of Problems, Issues, and Situations Encountered:

- The position routinely encounters complex problems related to the confidentiality, integrity, and availability of health information within the health system. Typical issues include security incidents, policy adherence, threat and risk assessments, and exceptions to security policies.
- The environment includes established provincial policies, standards, and legislation that guide the implementation and monitoring of security controls.

Steps to Resolve Problems and Independence:

- The Senior Security Analyst develops, implements, maintains, and monitors health system information security consistent with provincial policies and standards.
- They work collaboratively with IT project teams to vet project deliverables, complete Threat and Risk Assessments, and assist in making informed decisions to mitigate security risks.
- The position exercises considerable independence in leading the provincial information security incident response process and researching new tools and techniques to assess security controls.

Internal and External Stakeholders Impacted:

- The position impacts both technical and non-technical staff within the unit, the Department, and various health sector organizations.
- Stakeholders include provincial custodians connecting to the health systems, business areas requesting

exceptions, and the provincial stakeholder group for vetting security policies.

Size and Variety of Projects, Programs, Services Delivered or Supported:

- The Senior Security Analyst supports a variety of projects, security incident response, and the integration of new security tools into the Security Management program.
- They handle enquiries from business areas on unique scenarios and collaborate with provincial stakeholders to vet security policies, standards, and procedures.

Response to/Resolution of Problems/Issues:

- Leading the provincial information security incident response process.
- Researching and integrating new tools and techniques into the Security Management program.
- Collaborating with IT project teams and provincial stakeholders to ensure appropriate security measures are in place.

Variety of Problems and Solutions:

- The position deals with a variety of problems, from security incidents to policy adherence and risk assessments.
- Solutions often require creative thinking and collaboration with supervisors, colleagues, and documented guidelines.

Types of guidance available for problem solving:

- Security tools and services available from within the Health System Cybersecurity and Privacy Operations Unit.
- Security tools and services available from GoA CISO.

Direct or indirect impacts of decisions:

Position is an expert in identifying and mitigating information technology security risks and is required to influence policy and systems design. Position influences managers, executives, physicians and other clinicians, and those involved in designing and building healthcare systems internal and external to Alberta Health.

Key Relationships

Major stakeholders and purpose of interactions:

The Senior Security Analyst collaborates internally with the Manager, Privacy and Security for discussions, work assignments, and issue escalation; with the Director, Health System Cybersecurity and Privacy Operations for work status updates and further issue escalation; and liaises with the Executive Director to offer policy, strategy and progress updates, while also providing status updates to the ADM.

The position supports various program areas within the department to ensure comprehensive information security measures are in place and provide advice to other divisions as needed.

Externally, the analyst works with custodians to address security issues and participates in key GoA initiatives, providing feedback as required.

Required Education, Experience and Technical Competencies

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

If other, specify:

Computer & Information Security

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

Knowledge

Requires extensive knowledge of information security standards and practices, information security frameworks (ISO 27K,NIST, COBIT, etc.), Information Security testing tools and techniques, and privacy enhancing technologies. Also requires working knowledge of Health Information Act (HIA) and health specific principles and practices, including other relevant legislation compliance management.

Skills

In addition to technical skills, the incumbent requires well-developed oral and written communication skills, the ability to work independently and in a team environment, and experience with research and analysis to enhance knowledge of current and emerging trends within Information Systems Security.

Education

A degree in Information Systems Security Management or Information Technology with 3 years of related industry experience. In addition, the incumbent must have a recognized security industry certification like the Certified Information Systems Security Professional (CISSP) designation, or be able to demonstrate equivalent work experience.

Experience

In order to be able to perform the role, the incumbent must have technical and policy related experience in the Information security field in operational and tactical roles.

Requires a degree in Computing Science and 3 years of progressively responsible experience in computing and information security, including experience with Internet technology and security issues. Experience should include security policy development, security education, network penetration testing, application vulnerability assessments, risk analysis and compliance testing. CISSP, GIAC, or other security certifications desired.

Knowledge of information security standards (e.g., ISO 17799/27002, etc.), rules and regulations related to information security and data confidentiality (e.g., FERPA, HIA, etc.) and desktop, server, application, database, network security principles for risk identification and analysis are essential. Strong analytical and problem solving skills. Excellent communication (oral, written, presentation), interpersonal and consultative skills.

Behavioral Competencies

Pick 4-5 representative behavioral competencies and their level.

Competency	Level A B C D E	Level Definition	Examples of how this level best represents the job
Systems Thinking	○ ○ ○ ◉ ○	Integrates broader context into planning: • Plans for how current situation is affected by broader trends • Integrates issues, political environment and risks when considering possible actions • Supports organization vision and goals through strategy • Addresses behaviours	

		that challenge progress	
Creative Problem Solving	○ ○ ○ ◉ ○	Works in open teams to share ideas and process issues: • Uses wide range of techniques to break down problems • Allows others to think creatively and voice ideas • Brings the right people together to solve issues • Identifies new solutions for the organization	
Drive for Results	○ ○ ◉ ○ ○	Takes and delegates responsibility for outcomes: • Uses variety of resources to monitor own performance standards • Acknowledges even indirect responsibility • Commits to what is good for Albertans even if not immediately accepted • Reaches goals consistent with APS direction	

Benchmarks

List 1-2 potential comparable Government of Alberta: Benchmark

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