Alberta

Job Description

Public (when completed)

Common Government

New

Ministry

Technology and Innovation

Describe: Basic Job Details

Position

Position ID

Position Name (200 character maximum)

Information Security Officer 1, Work Experience Program

Requested Class

Systems Analyst Level 1

Job Focus

Supervisory Level

Agency (ministry) code

Cost Centre

Program Code: (enter if required)

Employee

Employee Name (or Vacant)

Organizational Structure

Division, Branch/Unit

☐ Current organizational chart attached?

Supervisor's Position ID

Supervisor's Position Name (30 characters)

Supervisor's Current Class

Design: Identify Job Duties and Value

Job Purpose and Organizational Context

Why the job exists:

Information Security Officers are tasked with the protection of the Government of Alberta's (GoA) information assets from a confidentiality, integrity, and availability perspective. They are responsible to identify, assess, monitor, detect, investigate, research, and respond to threats and incidents impacting the security of information assets.

The position is for the GOA's Work Experience Program (WEP), supports the GoA's Information Security Management Directives (ISMD) and contributes to the safe operation of the GoA computing environment. Key components of the WEP program include hands-on learning, personalized development plans, and dedicated mentorship. The program aims to bridge the gap between academic studies and the demand for professionals in the cybersecurity field, equipping participants with the skills and expertise needed to tackle real world challenges and excel in Alberta's growing cybersecurity industry. The Information Security Officer 1 is an entry level position. This level requires coaching and supervision from the upper levels.

Responsibilities

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

Responsibilities and Activities that may be assigned during the program

1. Governance, Strategy and Planning:
   - Assist in the delivery of the Information Security Program for the Government of Alberta and CyberAlberta.
   - Support compliance with GoA Information Security Management Directives, standards, and policies.
   - Participate in identifying information security requirements across programs and services.
2. Vulnerability, Threat Hunting, and Intelligence
   - Assist in identifying, assessing, and documenting information and technology security threats and risks.
   - Collect and analyze threat intelligence from multiple sources, including open-source intelligence (OSINT), commercial threat feeds, and internal data sources.
   - Contribute to the maintenance and improvement of threat hunting playbooks, procedures, and documentation.
   - Communicate relevant cyber vulnerabilities and threat information to technical and non-technical stakeholders, as required.
   - Collaborate with other security teams to support the integration of threat intelligence into security operations and incident response workflows.
3. Information Security Incident Monitoring, Investigation, and Response:
   - Monitor assigned incident tickets and alerts within security monitoring and ticketing systems.
   - Perform first-level security incident investigations under direct supervision and with appropriate clearance.
   - Assist in responding to suspected or confirmed information security incidents following established protocols.
   - Provide timely updates on incident status, actions taken, and resolution progress to service leads and management.
   - Complete security incident reports and support tracking, documentation, and continuous improvement processes.
4. Compliance Controls, and Risk Management:
   - Monitor compliance with information security policies, standards, and procedures, identifying deviations for review.
   - Stay informed of changes to relevant legislation, regulations, and standards (e.g., NIST, ISO 27001, privacy and security requirements) as directed.
   - Assist with risk assessments to identify, analyze, and prioritize information security risks.
   - Ensure identified risks are documented and maintained in the Government of Alberta Information Technology Security Risk Register.
   - Conduct research on cybersecurity threats, controls, and emerging risks to support service leads and decision-making.
5. Leverage Tools, Automation, and Artificial Intelligence to Enhance Security Practices
   - Assist in using data analytics, automation, and AI-enabled security tools to support reporting, threat analysis, incident triage, risk identification and other security related activities.
   - Contribute to documentation and analysis of AI-driven tools, including benefits, limitations, and governance considerations.
   - Apply responsible and ethical use principles when working with AI technologies, in alignment with GoA policies and guidelines.
   - Assist in identifying opportunities where automation or AI could improve repeatable security processes.
6. Security Awareness, Training, and Disaster Recovery Readiness
   - Participate in the development and maintenance of information security awareness and training materials.
   - Assist in tracking and reporting on training participation, completion rates, and effectiveness metrics.
   - Support disaster recovery (DR) planning activities, including documentation review and plan development.
   - Participate in disaster recovery testing exercises, simulations, and related issue tracking.

Problem Solving

Typical problems solved:

Types of guidance available for problem solving:

The successful candidate will have exposure to various areas of the Cybersecurity Division:

- Artificial Intelligence, Application & Product Security
- CyberAlberta Strategy & Planning
- Cybersecurity Awareness & Training
- Cybersecurity Enablement & Initiatives
- Cybersecurity Policies, Controls, & Compliance
- Cybersecurity Operations
- Digital Forensics
- IT Disaster Recovery

- Risk Management
- Threat Hunting
- Threat Intelligence
- Vulnerability & Zero Trust

Direct or indirect impacts of decisions:

Depending on circumstances, decisions may impact GoA systems and staff.

Key Relationships

Major stakeholders and purpose of interactions:

- Team Leaders, CISO, Director and Executive Director levels-interactions to collaborate, work on internal Business As Usual (BAU) cybersecurity tasks activities, projects, and initiatives
- Technology & Innovation departments, Other Ministry and Agencies-interactions to gain understanding of information technology processes and technologies and to direct or guide actions necessary to manage security related activities
- CyberAlberta Community of Interest and other external parties such as vendors, suppliers-interactions to guide or direct actions necessary to manage initiatives and external or 3rd party engagements and processes

Required Education, Experience and Technical Competencies

Education Level	Focus/Major	2nd Major/Minor if applicable	Designation
Diploma (2 year)	Other		

If other, specify:

Computer Science, IT or related

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

- Awareness of information security services and how to perform them, along with knowledge of some cyber security tools to perform these services including:
  - Governance, Strategy and Planning;
  - Threat Hunting and Intelligence;
  - Incident Monitoring, Detection, Investigation, and Response;
  - Audits, Compliance Controls, and Risk Management;
  - Information Security Awareness and Training;
  - Disaster Recovery
- A related two-year diploma in computer technology or related diploma from a recognized post-secondary institution. Equivalencies may be considered.
- A strong interest and/or foundational knowledge of information security practices, including threat and risk management, incident response, and forensic investigation.
- A cover letter clearly detailing how detailing how your skills and experience align with the responsibilities of the role. This will be used to assess intent, writing and communication skills.
- Relevant certifications in cybersecurity or related fields (e.g., CEH, Security+, CC, etc).

Equivalencies:

- A related one-year certificate from a recognized post-secondary institution and one year of related experience.

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
Agility	○ ◉ ○ ○ ○	Works in a changing environment and takes initiative to change: • Takes opportunities to improve work processes • Anticipates and adjusts behaviour to change • Remains optimistic, calm and composed in stressful situations	

		• Seeks advice and support to change appropriately • Works creatively within guidelines	
Build Collaborative Environments	◉ ○ ○ ○ ○	Works in an open honest manner with colleagues: • Creates sharing opportunities • Actively shares, accepts and listens to others • Recognizes conflict, respects and discusses opinions openly • Supports group even to learn from mistakes • Recognizes differing interpretations	
Creative Problem Solving	○ ◉ ○ ○ ○	Focuses on continuous improvement and increasing breadth of insight: • Asks questions to understand a problem • Looks for new ways to improve results and activities • Explores different work methods and what made projects successful; shares learning • Collects breadth of data and perspectives to make choices	
Systems Thinking	○ ◉ ○ ○ ○	Considers inter-relationships and emerging trends to attain goals: • Seeks insight on implications of different options • Analyzes long-term outcomes, focus on goals and values • Identifies unintended consequences	

Benchmarks

List 1-2 potential comparable Government of Alberta: Benchmark