New

Ministry

Technology and Innovation

Describe: Basic Job Details

Position

Position ID

Position Name (30 characters)

Information Security Officer 2

Requested Class

Systems Analyst Level 2

Job Focus

Corporate Services

Supervisory Level

00 - No Supervision

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:

Overall, 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 supports the GoA's Information Security Management Directives (ISMD) and contributes to the safe operation of the GoA computing environment. Incumbents may also be responsible for participating in or coordinating the development and implementation of security controls, including cyber security technology, processes, policy instruments, or awareness materials.

The Information Security Officer 2 position is the full working level of the position, which may be asked to mentor junior level resources.

Responsibilities

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

1. Leadership, advice, and planning:
   - Mentor and coach more junior staff
   - May be asked to lead or coordinate small project or set of activities

- Assist in delivery of the Information Security Program for the Government of Alberta
- Provide information security advice to stakeholders
- Participate in projects as an information security subject matter expert
- Participate in the identification of information security requirements, as well as the development of strategies and solutions to meet these requirements

2. Threat Intelligence and Risk Management:
   - Facilitate or perform identification, assessment, and treatment of information and technology security threats and risks
   - Ensure that risks are documented in the Government of Alberta's Information Technology Security Risk Register
   - Communicate cyber threat information to stakeholders as required
   - Perform cyber threat or cyber security controls related research as requested by Corporate Information Security Office management
3. Information Security Awareness and Training:
   - Participate in the development of awareness or training material as directed by Corporate Information Security Office management, or by GoA Communications staff
   - Plan, develop and implement the annual Cyber Security Awareness Month campaign for the Government of Alberta
   - Develop IT security communication materials as required
4. IMT Disaster Recovery:
   - Participate in disaster recovery testing exercises, which may include responding to related issues and incidents, assisting with test communication, or creating test scenarios for the exercises
5. Digital Investigations
   - Digital forensic examinations across the GoA computing environment.
   - Interact with CISO and Directing Counsel, responding to requests for forensic examinations and detailed/summary reports.
   - Represent CISO in reporting digital forensic examination findings with HR, Directing Counsel, and ministry line management.

Problem Solving

Typical problems solved:

Provision of Information Security Services:
- Advisory and planning services
- Threat Intelligence and Risk Management
- Information Security Incident Monitoring and Response
- Information Security Awareness and Training
- IMT Disaster Recovery

Types of guidance available for problem solving:

Security tools available within the CISO:
- Network security devices (i.e. Firewalls, Network Intrusion, Web Threat Management, SIEM)
- Digital Forensic software (i.e. Encase)
- Course authoring tools (i.e. Articulate Storyline 360)
- Graphic design tools (i.e. Adobe illustrator, photoshop)

Direct or indirect impacts of decisions:

Supported Stakeholders:
- The Government of Alberta, including all IMT Sectors, ministries and departments
- In some circumstances, may be directed by the Chief Information Security Officer to support services towards external agencies such as Legal counsel, Law Enforcement, Alberta Public Agencies or other organizations.

Key Relationships

Major stakeholders and purpose of interactions:

- Senior management, CISO (Director and Executive Director levels) - daily interaction to articulate security risks, methods and costs to manage security risks, present and support results of forensic analysis.
- Network and support analysts and managers (from Infrastructure Operations to Client Services) - daily interaction

to gain understanding of information technology processes and technologies and to direct or guide actions necessary to manage security risks or manage changes.

- Directing Counsel, Justice and Solicitor General - as required (based on forensic assignments) to receive instructions on actions required during the course of an investigation and to present facts and analysis gathered during the course of an investigation
- Digital Forensic Consultants - as required (based on forensic assignments) to oversee investigations, instructing consultants on GOA policies for investigations, providing day-to-day work instructions, reviewing work schedules and reports.
- Sector Information Security Officers -interaction as required to gain an understanding of IT processes and technologies and to guide or direct actions necessary to manage security risks or security awareness materials
- Ministry and Agency IT Support Staff (e.g. Ministries not using GOA Domain Services) -interaction as required to guide or direct actions necessary to manage awareness materials
- External agencies - as required (based on forensic assignments) and may include presenting evidence gathered during the course of an investigation to law enforcement or reviewing security risk advisories with other provincial governments or agencies.

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:

College diploma in a computer, information systems or information security related discipline.

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

University degree or college diploma in a computer, information systems or information security related discipline.

- Minimum of two (2) years of combined experience in information systems security, IT infrastructure planning, and/or IT architecture.
- One security certification (CISSP, CISM, CISA, CEH, GPEN, or equivalent) would be an asset, but more importantly, it is expected that incumbents would be working towards certification. Equivalences will be considered.
- Autonomy: ability to work under minimal supervision.
- Communication: excellent verbal and written communication skills are required to present detailed high-quality briefing material to executive management;
- Creative Problem Solving: ability to assess options and implications in new ways to achieve outcomes and solutions;
- Agility: to anticipate, assess, and quickly adapt to changing priorities, maintain resilience in uncertainty and effectively work in a changing environment;
- Develop Self: a commitment to lifelong learning and the desire to invest in the development of the long-term capability of yourself;
- Working knowledge of information security services and how to perform them, along with working knowledge of cyber security tools to perform these services including:
    - Incident monitoring, detection and response;
    - Threat and risk identification, assessment, treatment and management;
    - Information Security awareness and training
    - Digital forensic investigations;
    - IMT disaster recovery.

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	○ ○ ○ ○ ◉	Creates the environment for innovative problem solving: • Generates new ways of thinking; ensures right questions are being asked about a problem • Eliminates barriers to creativity and innovation • Encourages a culture of innovation	
Agility	○ ○ ○ ◉ ○	Proactively incorporates change into processes: • Creates opportunities for improvement • Is aware of and adapts to changing priorities • Remains objective under pressure and supports others to manage their emotions • Proactively explains impact of change on roles, and integrates change in existing work • Readily adapts plans and practices	
Drive for Results	○ ○ ○ ◉ ○	Works to remove barriers to outcomes, sticking to principles: • Forecasts and proactively addresses project challenges • Removes barriers to collaboration and achievement of outcomes • Upholds principles and confronts problems	

		directly • Considers complex factors and aligns solutions with broader organization mission	
Develop Networks	○ ○ ○ ◉ ○	Makes working with a wide range of parties an imperative: • Creates impactful relationships with the right people • Ensures needs of varying groups are represented • Goes beyond to meet stakeholder needs • Ensures all needs are heard and understood	
Build Collaborative Environments	○ ○ ○ ◉ ○	Involves a wide group of stakeholders when working on outcomes: • Involves stakeholders and shares resources • Positively resolves conflict through coaching and facilitated discussion • Uses enthusiasm to motivate and guide others • Acknowledges and works with diverse perspectives for achieving outcomes	
Develop Self and Others	○ ○ ○ ◉ ○	Encourages development and integration of emerging methods: • Shapes group learning for team development • Employs emerging methods towards goals • Creates a shared learning environment • Works with individuals to develop personal development plans	

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
ADM Name	Date yyyy-mm-dd	ADM Signature
DM Name	Date yyyy-mm-dd	DM Signature