New

Ministry

Technology and Innovation

Describe: Basic Job Details

Position

Position ID

Position Name (30 characters)

Information Security Officer 3

Requested Class

Systems Analyst Level 3

Job Focus

Corporate Services

Supervisory Level

Agency (ministry) code

Cost Centre

Program Code: (enter if required)

Employee

Employee Name (or Vacant)

VACANT

Organizational Structure

Division, Branch/Unit

Cybersecurity/Cybersecurity Services

☐ 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 3 position is the senior working level of the position. An incumbent may be asked to lead a team, an activity or a project relating to information security.

Responsibilities

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

1. Leadership, advice, and planning:
   - May act as a service team lead, supervising direct reports assigned to the service team and delegating tasks and service requests to reporting staff.
   - Mentor and coach more junior staff.

- May be asked to lead or coordinate small project or set of activities.
- Assist in the planning and delivery of the Information Security Program for the Government of Alberta.
- Assist in facilitating compliance to the Government of Alberta's Information Security Management Directives.
- Provide information security advice to stakeholders.
- Participate in projects as an information security subject matter expert.
- Participate in the development and implementation of information security policies, strategies, processes and other controls in compliance with Government of Alberta Information Security Management Directives and Standards.
- 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 Cybersecurity Services management.
   - Analyze threat and risk information and trends to formulate recommendations to improve the Government of Alberta's security posture.
3. Information Security Incident Monitoring and Response:
   - Monitor incident tickets that may be assigned to the team.
   - Participate in on call information security incident support rotation.
   - Respond to information security incidents as required, following established procedures and protocols.
   - Manage critical or escalated incident responses, which may involve managing a small incident response team.
   - Provide updates regarding incident response and resolution to management.
   - Complete Information Security Incident reports and submit to the Cybersecurity Services management.
4. Digital Forensic Investigations:
   - Perform and lead digital forensic investigations, as directed by Legal Services or by the Chief Information Security Officer, in the event of suspicious activities, suspected or confirmed information breaches, and identified security incidents.
   - Review investigation requirements with requestor.
   - Work with on-site personnel to gain physical and computer access for forensic data/evidence gathering.
   - Document all steps in evidence gathering and handling.
   - Complete analysis of evidence, escalating anomalies or other investigative issues to Directing Counsel immediately.
   - Maintain currency of computer forensic investigation and analysis skills through independent research and training.
   - Document reports that will be presented as evidence during disciplinary hearings and potentially criminal or civil proceedings with precise attention to detail for Directing Counsel.
   - Present results of investigation to Directing Counsel and/or Ministry senior management.
5. Information Security Awareness and Training:
   - Participate in the development of awareness or training material as directed by Cybersecurity Services management.
   - Facilitate in-class awareness or training sessions using previously developed information security awareness or training material.
6. IMT Disaster Recovery:
   - Participate in disaster recovery planning activities, including the facilitation of disaster recovery plan development;
   - Participate in disaster recovery testing exercises, which may include planning the tests or responding to related issues and incidents, assisting with test communication, or coordinating particular test activities.
   - Participate in actual disaster recovery exercises including responding to related issues and incidents, assisting with test communication, or coordinating particular test activities.

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
- Digital Forensic Investigation
- Information Security Awareness and Training
- IMT Disaster Recovery

Leadership:

- Mentor and coach more junior staff
- May act as a service team lead and supervisor for direct reports on the service team
- May manage and coordinate projects or sets of activities

Types of guidance available for problem solving:

Guidance documents for problem solving:

- GoA's Information Security Management Directives (ISMD)
- GoA IMT Policy Instruments.
- Other Cybersecurity Services documentation.

Direct or indirect impacts of decisions:

- Depending on circumstances, decisions may significantly impact Goa staff.

Key Relationships

Major stakeholders and purpose of interactions:

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.
- Ministry and Agency IT Support Staff (e.g. Ministries not using GOA Domain Services) - daily interaction 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:

computer, information systems or information security related discipline.

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

Education and Certification:

- University degree or college diploma in a computer, information systems or information security related discipline.
- Minimum of three (3) 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) is a desirable asset, and it is expected that incumbents would be working towards multiple certifications.
  Equivalencies will be considered.

Knowledge, Skills & Abilities:

- Autonomy: ability to work independently or under minimal supervision.
- Leadership: ability to lead and remain calm in times of crisis is an absolute mandatory skill;
- Communication: excellent verbal and written communication skills are required to present detailed high-quality briefing material to executive management;
- Systems Thinking: ability to keep broader impacts and connections in mind;
- Creative Problem Solving: ability to assess options and implications in new ways to achieve outcomes and solutions;
- Drive for Results: knowing what outcomes are important and maximizing resources to achieve results that are aligned with the goals of the organization, while maintaining accountability to each other and external stakeholders;
- 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;
- In depth knowledge of information security services and how to perform them, along with working knowledge of cyber security tools to perform these services including:
  - Threat and risk identification, assessment, treatment and management;
  - Incident monitoring, detection and response;
  - Digital forensic investigations;
  - Information Security awareness and training;
  - 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	○ ○ ◉ ○ ○	Identifies and manages required change and the associated risks: • Identifies alternative approaches and supports others to do the same • Proactively explains impact of changes • Anticipates and mitigates emotions of others • Anticipates obstacles and stays focused on goals • Makes decisions and	

		takes action in uncertain situations and creates a backup plan	
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	
Drive for Results	○ ○ ○ ○ ◉	Aligns different groups to achieve goals and realize broader outcomes: • Defines work mission to achieve APS goals and integrate projects • Provides bold advice to stakeholders • Proactively improves overall performance, measured through metrics	
Develop Networks	○ ○ ○ ○ ◉	Builds trust to fairly represent every party: • Uses network to identify opportunities • Establishes credibility and common purpose with a range of people • Actively represents needs and varying groups • Creates strategic impression by inspiring and connecting with values and beliefs	
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