Government of Alberta

NON-MANAGEMENT JOB DESCRIPTION
POINT RATING EVALUATION PLAN

Working Title	Name
Information Security Officer 3	

Position Number	Reports to Position No., Class & Level	Division, Branch/Unit	Ministry
		OCCIO&T/Cybersecurity Services	Service Alberta

Present Class	Requested Class

Dept ID	Program Code	Project Code (if applicable)

PURPOSE: Give a brief summary of the job, covering the main responsibilities, the framework within which the job has to operate and the main contribution to the organization (see Non-Management Job Description Writing Guide **Pages 7-8**).

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 AND ACTIVITIES: The purpose of the job can be broken down in different responsibilities and end results. Each end result shows what the job is accountable for, within what framework and what the added value is. Normally a job has 4-8 core end results. For each end result, approximately 3-6 activities should be described (see Writing Guide **Pages 9-10**).

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 Corporate Information Security Office 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.

RESPONSIBILITIES AND ACTIVITIES: The purpose of the job can be broken down in different responsibilities and end results. Each end result shows what the job is accountable for, within what framework and what the added value is. Normally a job has 4-8 core end results. For each end result, approximately 3-6 activities should be described (see Writing Guide **Pages 9-10**).

- 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 Corporate Information Security Office.

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 Corporate Information Security Office 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.

SCOPE: List specific information that illustrates the challenges, problem solving and creativity requirements and decision making capacity of the position. Also identify the internal or external areas the job impacts (see Writing Guide **Pages 11-12**).

Scope:

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.

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

KNOWLEDGE, SKILLS & ABILITIES: Include information on required diplomas and degrees along with identifying the most important knowledge factors, including knowledge about practical procedures, administrative, technical or professional techniques, technical, scientific or program related processes, etc. Detail specific training if there is an occupational certification/registration requirement for the position. Specify the type of experience required for the position (see Writing Guide **Pages 12-14**).

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

Education and Certification:

- University degree or college diploma in a computer, information systems or information security related discipline.
- Minimum of three (4) 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.

CONTACTS: Identify the main contacts the position communicates with and the purpose of the communication (See Writing Guide **Pages 14-15**).

- 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 Service Provisioning, Service Delivery and Network Services and ICT Suppliers), Service Alberta – 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.
- Ministry or Sector based Information Security Officers – daily interaction to gain an understanding of information technology 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) – 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.

SUPERVISION EXERCISED: List position numbers, class titles, and working titles of positions directly supervised (see Writing Guide **Page 15**)

Directly supervise and coach more junior staff, including Information Security Officers 1 and 2. May be assigned team leadership, or project coordination duties.

CHANGES SINCE LAST CLASSIFICATION REVIEW: Identify significant changes, that have impacted the responsibilities assigned to your position since the last review (see Writing Guide **Pages 15-16**).

ORGANIZATION CHART: An organization chart that includes supervisor, peers and staff **MUST** be attached (see Writing Guide **Page 17**).

This information is being collected under the authority of Section 10 of the Public Service Act and will be used to allocate positions within a classification plan and to manage the Alberta government human resources program. If you have any questions about the collection of this information, contact the Job Evaluation Unit, 6th Floor, Peace Hills Trust Tower, 10011 - 109 Street, Edmonton, Alberta, T5J 3S8, phone 780/408-8400 or contact your Ministry Human Resource Office.

Signatures

The signatures below indicate that the incumbent, manager and division director/ADM have read, discussed and agreed that the information accurately reflects the work assigned (see Writing Guide **Page 16**)

	Name	Signature	Date
Director			
Executive Director			
Division Director/ADM			
Executive Director - HR			
DM			