JOB DESCRIPTION

POINT RATING EVALUATION PLAN

|  |  |
| --- | --- |
| Working Title | Name |
| Info Sec Officer 1 |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Position Number | Reports to Position No., Class & Level | Division, Branch/Unit | Ministry |
|  |  | Cybersecurity Services/CyberAlberta | Technology & Innovation |

|  |  |
| --- | --- |
| Present Class | Requested Class |
| System Analyst 1(511SAA) |  |

|  |  |  |
| --- | --- | --- |
| 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 [**Section 2.3**](http://www.chr.alberta.ca/class/forms/write-job-description/how-to-write-job-descr.htm#step3)). |
| --- |
| 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 is for the GOA’s Work Experience Program (WEP) and 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 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 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 major activities should be described (see [**Sections 2.1**](http://www.chr.alberta.ca/class/forms/write-job-description/how-to-write-job-descr.htm#step1) and [**2.2**](http://www.chr.alberta.ca/class/forms/write-job-description/how-to-write-job-descr.htm#Step2)). |
| --- |
| **Responsibilities and Activities that may be assigned during the program**   1. Governance, Strategy and Planning:    * Assist in delivery of the Information Security Program for the Government of Alberta and CyberAlberta    * Assist in facilitating compliance to the Government of Alberta’s Information Security Management Directives    * Participate in the identification of information security requirements, as well as the development of strategies and solutions to meet these requirements 2. Threat Hunting and Intelligence    * Perform identification, assessment, and treatment of information and technology security threats and risks    * Collect and analyze threat intelligence from various sources, including open-source intelligence (OSINT), commercial threat feeds, and internal data.    * Contribute to and maintain threat hunting playbooks and procedures to standardize and streamline activities.    * Communicate cyber threat information to stakeholders as required    * Work closely with other security teams to integrate threat intelligence into security operations and incident response processes. 3. Information Security Incident Monitoring, Investigation, and Response:    * Monitor incident tickets that may be assigned to the team    * Perform 1st level digital forensic investigations under direct service lead supervision with legal and CISO clearance in the event of suspicious activities, suspected or confirmed information breaches, and identified security incidents.    * Respond to information security incidents as required, following established procedures and protocols.    * Provide updates regarding incident response and resolution to management.    * Complete security incident reports and submit for tracking and recording 4. Compliance Controls, and Risk Management:  * Monitor compliance with security policies and procedures, identifying and addressing any deviations. * Stay informed about changes in relevant laws, regulations, and standards (e.g., GDPR, HIPAA, ISO 27001) and ensure organizational compliance * Conduct regular risk assessments to identify, evaluate, and prioritize information security risks. * Ensure that risks are documented in the Government of Alberta’s Information Technology Security Risk Register * Perform cyber threat or cyber security controls related research as requested by service leads.  1. Information Security Awareness and Training:    * Participate in the development of awareness or training material.    * Help track and report on training participation and effectiveness, using metrics to identify areas for improvement. 2. 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 responding to related issues and incidents    * Participate in actual disaster recovery exercises for internal and external GOA when applicable |

| **SCOPE:** List specific information that illustrates what internal or external areas the job impacts, and the diversity, complexity, and creativity of the job (see [**Section 2.4**](http://www.chr.alberta.ca/class/forms/write-job-description/how-to-write-job-descr.htm#Step4)). |
| --- |
| Supported Stakeholders:   * The Government of Alberta, including various ministries and departments. * The CyberAlberta Community of Interest (COI) members in some circumstances, events, and initiatives. * Maybe 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.   The successful candidate will have exposure to the following areas of the Cybersecurity Division:   * 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 & Reporting * Vulnerability & Zero-Trust |

| **KNOWLEDGE, SKILLS & ABILITIES:** Provide a list of diplomas, degrees and the most important knowledge factors, skills and abilities including knowledge about practical procedures, specialized techniques, etc.; analytical and conceptual skills and abilities; and skills needed for direct interaction with others. Specific training if it is an occupational certification/registration required for the job. |
| --- |
| * Autonomy: The ideal candidate should be able to take initiative and demonstrate a strong sense of responsibility, would be working under direct supervision from a service lead. * Creative Problem Solving: Ability to analyze complex security issues, identify potential threats, 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. * 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 |
|  |

| **CONTACTS:** The main contacts of this position and the purpose of those contacts. |
| --- |
| * 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 |

| **SUPERVISION EXERCISED:** List position numbers, class titles, and working titles of positions directly supervised. |
| --- |
| No direct supervision. |

| **CHANGES SINCE LAST CLASSIFICATION REVIEW:** List the significant changes that have occurred in your job since the last review. |
| --- |
|  |

|  |
| --- |
| **ORGANIZATION CHART:** An organization chart that includes supervisor, peers and staff **MUST** be attached. |

***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.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Manager |  |  |  |  |  |
|  | Name | Signature | Date |
| **Director** |  |  |  |
|  | Name | Signature | Date |
| Division Director/ADM | S |  |  |
|  | Name | Signature | Date |
| Executive Director - HR |  |  |  |  |  |
|  | Name |  | Signature |  | Date |
| DM |  |  |  |  |  |
|  | Name |  | Signature |  | Date |