Justice Institute
BRITISH COLUMBIA

JOB POSTING

Date: December 14, 2023
Competition: 23-112

APPLICATIONS ARE INVITED FOR THE FOLLOWING FULL-TIME REGULAR POSITION

Position:	**Cyber Security Manager (Position #1000385)**
Division:	**Technology Services**
Reporting To:	**CIO, Technology Services**

Justice Institute of British Columbia:

The Justice Institute of British Columbia (JIBC) is a public, post-secondary institution that provides education and training to those who'll be there to support British Columbians and others around the world, when a life is at stake or when health, safety or property is in jeopardy. Work for JIBC and be a part of the big picture – supporting justice and public safety professionals at all stages of their careers in fields including law enforcement, firefighting, paramedicine, security and emergency management.

Position Summary:

The Cyber Security Manager will be dedicated to managing all aspects of information security, including working with people, processes, and technologies internally as well as with partner organizations to protect JIBC from cyber threats and build a culture of security awareness within JIBC. The dedicated role will ensure consistent application of cyber security controls across all technologies, as well as manage the nontechnical aspects of information security.

Primary Responsibilities:

Governance, Risk, and Compliance

- Manages and champions an ongoing information security awareness program with the goal of building a culture of cyber-awareness across JIBC, including awareness campaigns, training, and engagement initiatives.
- Builds increased information security capacity and awareness across the Technology Services team.
- Develops, recommends, monitors, and enforces JIBC's information security policies, baselines, standards, and procedures.
- Coordinates the documentation, categorization, and mitigation of security risks.
- Provides leadership, direction, and mentoring to team members and external resources.
- Evaluates JIBC's information security posture against established cybersecurity frameworks (e.g., Defensible Security, NIST, CIS Controls) and identify gaps and priority areas for improvement.
- Builds relationships with other institutions and organizations to maximize efficiency of JIBC's information security efforts through collaboration and information sharing.

Security Engineering, Architecture, and Testing

- Designs, develops, and implements information security systems and architecture.

- Operates a vulnerability management program for JIBC, including ongoing vulnerability assessments, analysis, prioritization, and coordination of remediation efforts.
- Audits and validates the security of JIBC systems via penetration tests, threat hunting, active countermeasures, adversary emulation, etc.
- Conducts tabletop exercises and tests to support the effectiveness of security controls.
- Leads the development, coordination, and implementation of large and/or complex cyber security related projects.

Information Security Operations

- Provides advisory services and support regarding the administration of operational security IT systems, i.e., endpoint detection and response (EDR), identity and access management (IAM), systems management/patch management, and firewalls.
- Manages the collection, analysis and correlation of security-related data and events from various sources within JIBC's IT infrastructure.
- Leads incident response and remediation of information security incidents, including root cause analysis and integrating lessons learned into future practices.
- Plans, manages, and communicates systems and initiatives that build efficiency and/or contribute to improved cybersecurity maturity.
- Manages the implementation of safeguards and countermeasures to support JIBC's information security posture.
- Manages cybersecurity contracts and maintains relations with cybersecurity vendors.
- Manages and implements shared security services from BCNET, CANARIE, and other shared service organizations.
- Remains informed of information security and technology developments and best practices through research, training, and attendance at infosec/IT events.

Qualifications & Requirements:

Academic:

- A bachelor's degree in a Computer Science, Information Technology, Engineering, MIS or equivalent. An equivalent combination of education, training and experience may be considered.
- Professional certifications such as CISSP, Security+, CEH, CISM, or CISA.

Other Knowledge/Training:

Knowledge, Skills and Abilities

- Proven experience in information security management, preferably in a leadership role.
- Strong knowledge of information security technologies, tools, and best practices.
- Excellent communication and leadership skills.
- Ability to work collaboratively with cross-functional teams.
- Exceptional interpersonal skills including the ability to negotiate and influence others.
- Exceptional oral and written communication skills and demonstrated ability to establish and maintain collaborative working relationships with co-workers, other staff, consultants and contractors.

- Self-directed with a high degree of initiative and confidentiality and ability to function as a team player.
- Ability to think innovatively and creatively in planning and developing a fresh approach to existing activities, with a continuous improvement perspective and incorporating best practices.
- Ability to make sound decisions under pressure and in response to security incidents.

Related Experience:

- 5+ years of experience working in an information security related discipline.
- Experience managing complex IT/cybersecurity projects.
- Experience in assessing enterprise risk from cybersecurity perspective.
- Experience in assessing multi-vendor cloud environments (AWS, Azure, GCP) and awareness of their security offerings.
- Experience in using application security testing, as well as penetration testing.
- Experience working in post-secondary or other public sector environments.

We offer a total compensation package that includes a benefit plan, which includes Extended Health and Dental Benefits after three months, and enrollment in the College Pension Plan upon hire. In addition, we offer 20 vacation days and 10 Personal Days annually (pro-rated in first year), as well as generous other leave entitlements.

Salary Range: **$87,729.35 to $103,211 annually – Fair Comparison Excluded Compensation Salary Grid 9**

The Compensation Range shown reflects JIBC's range for the role: between 85% and 100% of the sector range control point. In the normal course, employees will be hired, transferred or promoted between 85% - 94% of the control point, based on the knowledge, qualifications and experience for the role, with exceptions in the 95% - 100% range.

Position is under review to be determined for exclusion.

Posting Date: **December 14, 2023**
Closing Date: **Open until filled with a first review of candidates on January 2, 2024**

Please submit a *resume, covering letter and copies of academic credentials*, quoting Competition #23-112 via email to: People and Culture at hr@jibc.ca

For more information about this position, please contact: Peter Gregorowicz at pgregorowicz@jibc.ca.

Justice Institute of British Columbia believes in creating accessible programming, workplaces and spaces that reflect the community we serve. Our desire is to continue to build an inclusive culture that encourages, supports, and celebrates the diverse voices of our employees and students and where everyone feels empowered to share their experiences and ideas.

We encourage applications from members of groups that have been marginalized on any grounds named under the B.C. Human Rights Code, including sex, sexual orientation, gender identity or expression, racialization, disability, political belief, religion, marital or family status, age, and/or a person of Indigenous ancestry.

Justice Institute

BRITISH COLUMBIA

LEARNING THAT TAKES YOU BEYOND