



JOB DESCRIPTION

We at Kwantlen Polytechnic University respectfully acknowledge that we live, work and study in a region that overlaps with the unceded traditional and ancestral First Nations territories of the Musqueam, Katzie, Semiahmoo, Tsawwassen, Qayqayt, and Kwikwetlem, and with the lands of the Kwantlen First Nation, which gifted its name to this university.

POSITION TITLE: Director, Information Security

DEPARTMENT: Information Technology

DATE CREATED: September 2018

DIVISION/FACULTY: Finance & Administration

DATE REVISED: June 2026

ORGANIZATIONAL STRUCTURE

This role reports to the Chief Information Officer, Information Technology. Reporting directly to this position are IT team members responsible for technical information security technologies including incident management teams.

PRIMARY FUNCTION

The Director Information Security is responsible for leading the development, enforcement, and maintenance of policies, procedures, measures, and mechanisms to protect the confidentiality, integrity and availability of the University's information systems and data. The role requires translating the IT-risk requirements and business objectives into technical control requirements and specifications.

The Director will be required to provide leadership and will work with the IT organization and business management to align priorities and plans with key business objectives. The Director of Information Security is also responsible for working with business and IT constituents to balance real-world risks with business drivers such as speed, agility, flexibility, and performance. The Director will lead strategic security focused projects and oversee security related initiatives. This position will lead the introduction and implementation of security and protection of information and data planning for all divisions and business operations across the University.

KEY RESPONSIBILITIES

Leadership and Management

1. Supervises and provides leadership to direct reports by coaching and modeling key behaviours/strategies, encouraging dialogue and providing guidance and advice to facilitate resolutions to work issues. Assists team members to define shared and individual goals, meet target dates and ensure alignment of team goals. Monitors and assesses performance.
2. Contributes to effective employee and labour relations by administering the collective agreement(s), representing management in the grievance process and consulting with Labour Relations regarding collective agreement interpretation, as appropriate.



3. Provides leadership, vision, and guidance to the IT team, divisional business units, and faculties, ensuring their collective contribution towards achieving the Institutional Information Security Program.
4. Works with the CIO and IT leaders, to develop an overall information security strategy in the context of the IT strategic plan and University's vision.
5. Provides regular reporting to the KPU Board of Directors on Information Security matters and risk mitigation initiatives.
6. Develops productive relationships with business and academic leaders across the University to influence how sound Information security practices and protections can be integrated into their daily operations.
7. Develops, leads and enhances Information Security Awareness training programs with Human Resources to ensure all KPU employees are aware of the many cyber threats and to have the awareness to mitigate the risks.
8. Manages relationships with Information Security related vendors and cloud service providers to ensure they cost-effectively and securely meet the needs of the University.
9. Leads a University Incident Management team to manage and mitigate large scale Information Security breaches.

Budgeting, Finance and Administration

10. Formulates detailed financial targets for the University Information Security program and annual operating budget; also manages expenses to stay within plan. Establishes financial discipline in creating and achieving budget plans.

Strategic Support

11. Leads the development of the University security program and security projects that address identified risks, areas of vulnerability and business security requirements.
12. Manages the process of gathering, analyzing, and assessing the current and future threat landscape, as well as providing the CIO with a realistic overview of vulnerabilities, risks and threats in the enterprise environment.
13. Monitors and ensures compliance with relevant data protection laws and industry regulations. Conducts regular audits to assess compliance with security policies.
14. Develops and implements security-related policies, which serve as the foundation for safeguarding KPU's data and information systems. Aligning the KPU Information Security Strategy with B.C. Provincial Governments information Security Policy.

Security Liaison

15. Ensures security communication, awareness and training for various audiences including resource owners, mid-senior leadership and field staff.
16. Assists resource owners and IT staff in understanding and responding to security audit failures.



17. Liaises with vendors and the legal and purchasing departments to establish mutually acceptable contracts and service-level agreements.
18. Manages production issues and incidents and participate in problem and change management forums.
19. Serves as an active and consistent participant in the information security and protection governance process.
20. Works with the CIO and IT and relevant key parties to define metrics and reporting strategies that effectively communicate successes and progress of the security program.
21. Provides support and guidance for legal and regulatory compliance efforts, including audit support.

Architecture/Engineering Support

22. Consults with IT managers and project leaders to ensure that security is factored into the evaluation, selection, installation and configuration of hardware, applications, and software.
23. Validates that the security and IT teams have applied the required technical controls in support of established security policies.
24. Works with the Enterprise Architecture team to ensure that there is convergence of business, technical and security requirements; liaise with IT management to align existing technical installed base and skills with future architectural requirements.
25. Develops strong working relationship with the Office of General Counsel and Organizational Risk to develop and implement controls and configurations aligned with security policies and legal, regulatory and audit requirements. Develop strong working relationships with information application owners, mid-senior leadership, and staff to achieve buy-in in the development and implementation of controls and configurations that align with security policies and legal, regulatory and audit requirements.

Cloud Information Security

26. Develops and maintains an Information Security assessment framework for perspective cloud vendors. This is to ensure vendor security protections meet or exceed KPU Information security and privacy requirements.
27. Develops and maintains an audit schedule of contracted cloud vendors to ensure KPU data and processes are secured appropriately throughout the contract duration.

Incident Management Program

28. Develops, leads, and maintains in consultation with KPU's vendor partners an enterprise Incident Management program. This program and team will be activated in case of an Information Security Incident or Privacy breach.

Operational Support

29. Coordinates, measures and reports on the technical aspects of security management.



30. Oversees vendor management that provides information security functions for compliance with contracted service-level agreements.
31. Provides leadership and strategic direction for the KPU Cyber incident management program.
32. Consults with Human Resource Services and division or faculty leaders to identify an appropriate approach if incident source is deemed employee related.
33. Develops and establishes the strategic framework for threat and vulnerability management, set risk tolerances, formulate treatment plans, and ensure effective communication of residual risk information across the university.
34. Provides strategic direction and oversight for the periodic review of audit trails, system logs, and other monitoring data sources to maintain compliance with policies and audit requirements, ensuring alignment with the organization's security and compliance objectives.
35. Oversees and ensures security testing procedures are ongoing to verify the security of systems, networks, and applications, and the remediation of identified risks.
36. Establishes a high personal standard of service and performance by actively participating in other duties as assigned, education seminars, training programs, etc.
37. Contributes to and promotes a safe, equitable, respectful, and inclusive work environment by adhering to university policies and procedures and completing mandatory training programs.

QUALIFICATIONS

EDUCATION & EXPERIENCE

- Bachelor's degree in information system;
- A minimum of seven years of IT experience, with five years in an information security role and at least two years in a supervisory capacity;
- Certified Information Systems Security Professional (CISSP) information security is preferred;
- Or an equivalent combination of education, training and experience.

KNOWLEDGE, SKILLS and ABILITIES

- Proven expertise in Identifying, assessing, and prioritizing information security risks. Implement risk mitigation measures and ensure compliance with relevant regulations and standards.
- Strong leadership persuasion abilities and experience working with the risk management team and a variety of diverse business units. Strong project management skills and experience in creating and managing complex project plans, including budgeting and resource allocation.
- Demonstrated experience working with security tools, technologies, mechanisms and policy to support and protect business information infrastructure in a large organization.



An understanding of operating system internals and network protocols. Familiarity with the principles of cryptography and cryptanalysis.

- Knowledge and experience in developing and documenting security architecture and plans, including strategic, tactical and project plans.
- Experience developing and maintaining policies, procedures, standards and guidelines using a consultative and inclusive approach.
- Experience with common information security management frameworks.
- Experience in application technology security testing (white box, black box and code review) and in system technology security testing (vulnerability scanning and penetration testing).
- Familiarity with applicable legal and regulatory requirements for post-secondary education in the Province of British Columbia.
- Proven ability to communicate security technical concepts to nontechnical people to enhance understanding and drive decisions that lead to positive outcomes.
- Proficiency in performing risk, business impact, control, and vulnerability assessments, and in defining treatment of strategies.
- Excellent verbal, written and interpersonal communication skills, including the ability to communicate effectively with the IT organization, project and application development teams, management and business personnel and other internal and external University stakeholders.
- Ability to travel between campuses is required.

COMPETENCIES

- **Leadership:** KPU employees inspire, coach, mentor, and support students, employees and KPU as a whole in achieving objectives.
- **Accountability:** KPU employees demonstrate fiscal accountability and take ownership for their actions, decisions and results.
- **Continuous Improvement:** KPU employees take a creative approach to opportunities, exploring unique ways to create optimal value for the KPU community.
- **Collaboration:** KPU employees work in functional and cross-functional teams, coming together to solve complex issues and accomplish objectives that will benefit the KPU community.