



# THE UNIVERSITY OF WINNIPEG

## Chief Information Security Officer (CISO) – *new role*

Located in downtown Winnipeg, Manitoba, and on original Treaty One land, in the heart of the Métis homeland, The University of Winnipeg offers high-quality undergraduate and graduate programs in Arts, Business and Economics, Education, Kinesiology and Applied Health, and Science. The University is home to approximately 10,000 undergraduate and graduate students, 340 full-time faculty, 323 instructional staff, and 489 support staff. It has an established reputation for providing a supportive learning and working environment, combining a commitment to academic and research excellence, dedication to Indigenous engagement and success, and connections with diverse communities.

### The Opportunity

This is a new position that will report to the Vice President Finance and Administration (VPFA). The Chief Information Security Officer (CISO) will collaborate with the CIO and Senior Administration to define objectives for information security to safeguard against unauthorized access to university data and related computing resources. The CISO will work closely with the Technology Sector, senior administration, academic leaders, and the campus community to deliver a comprehensive information security strategy and create/inform the appropriate policies to manage information security risks.

### Accountabilities

- Oversee the formation and operation of university-wide information security (IS) resources and serve as an advisor on issues related to policy, legislation, regulations, and security technology deployment.
- Stay abreast of IS issues affecting higher education provincially and nationally and lead consultation with other peripheral partners including federal and provincial governments, external consultants, and other industry collaborators as appropriate on required security matters or assessments and audits as well as cyber security trends across other industries and internationally.
- Lead the development and implementation of information security policy instruments and practices to secure classified data to ensure legal and regulatory compliance.
- Spearhead efforts to internally assess, evaluate and make recommendations to administration regarding the adequacy of the security controls for the University's information and technology systems.
- Coordinate and track all security-related audits including scope areas involved, timelines, and outcomes. Provide guidance, evaluation, and advocacy on audit responses.
- Develop and maintain the cyber security incident response protocol, including the conduct of periodic table-top exercises to ensure a high-level of understanding and preparedness among all campus stakeholders.
- Use industry best practices, methods, and tools to coordinate vulnerability assessments and work with the campus management to enforce proper cyber security practices.
- Keep abreast of suspected or confirmed security incidents and be the response leader during cyber security incidents, coordinating the response activities and flow of information relating to the incident.
- Develop, implement and administer technical security standards, as well as a suite of security services and tools to address and mitigate security risk. Direct the assessment and evaluation of IS risks and monitor compliance with security standards and appropriate policies.
- Provide leadership, motivation, coaching, professional development and support to foster engagement and a focus on customer service.
- Manage, lead, and mentor IS Team members. Implement professional development plans for all team members in an environment conducive to staff development and training.

### Qualifications and Background

- A Master's Degree in Information Security, or other related field plus equivalent training and experience.
- Certified Information Systems Security Professional (CISSP) or equivalent.
- Minimum 10 years' progressively responsible experience in computing and information security, network security issues, and security incident response or related information technology fields, preferably in a higher education or equivalent complex environment.
- Minimum 5 years of experience in leadership and people management.
- Experience developing and administering an IS program and IS policy and regulations in a complex environment.
- Expertise in cyber security, in strategic planning, change management, resource management and reporting.

**To apply submit a cover letter and curriculum vitae, to [Jen@harrisleadership.com](mailto:Jen@harrisleadership.com) quoting project #25108.**

*The University of Winnipeg is committed to equity, diversity and inclusion and recognizes that a diverse staff and faculty benefits and enriches the work, learning and research environments, and is essential to academic and institutional excellence. We welcome applications from all qualified individuals and encourage women, racialized persons, Indigenous persons, persons with disabilities, and 2SLGBTQ+ persons to confidentially self-identify at time of application. All qualified candidates are encouraged to apply; however, Canadian citizens and permanent residents will be given priority. The University of Winnipeg is committed to ensuring employment opportunities are accessible for all applicants. If you require accommodation supports during the recruitment process, please contact [human\\_resources@uwinnipeg.ca](mailto:human_resources@uwinnipeg.ca).*