

EMPLOYMENT OPPORTUNITY

Women's College Hospital is the first and only independent, academic, ambulatory care hospital in Ontario with a primary focus on the health of women. If you're ready to be part of the future of healthcare, then you will want to join an institution in which the possibilities for creative innovation, breakthroughs in new thinking and groundbreaking work in academic ambulatory medicine are limitless. Women's College Hospital is committed to patient safety as a key professional value and an essential component of daily practice.

An exciting Regular Full-Time opportunity as a **Network & Security Engineer (Competition #193.18)** exists in Information Management/Information Technology reporting to the Manager, Technology Services. This role is responsible for identifying and articulating security risk and providing practical recommendations to management, providing plans for remediation of identified risks, implementing remediation and proactive fixes as necessary.

Summary of Duties, but not limited to:

- Regularly evaluates information security posture across technology solutions
- Produce high quality information security risk reports, clearly articulating risks and providing practical recommendations to senior management
- Regularly monitors compliance vs. internal/industry targets for KPIs
- Develops plans for remediation of any risks or issues identified, implements remediation or proactive fixes where applicable
- Assesses risk to the organization's information/technology assets based on evolving landscape (internal/external)
- Integrates information security principles into corporate initiatives, ensuring alignment and engagement with organizational stakeholders (such as privacy, health information, etc.)
- Participate in projects by evaluating requirements, interviewing stakeholders, providing security-related questions and feedback, evaluating technical solutions, managing security testing (including Vulnerability Assessments and Pen. Testing), producing appropriate reports, and following up on recommendations
- Provide expertise and oversight to ensure the organization adheres to corporate policies, minimizes risks and follows best practices to protect organizational resources
- Improve the efficiency and effectiveness of information security governance, security architecture, security procedures, standard practices, and technical standards
- Promote the understanding and adoption of information security standards, solutions, products and tools by both technical, clinical and business personnel
- Provide analysis and guidance regarding threats, vulnerabilities, and privacy and security incidents
- Provides hands-on support/guidance to WCH's technical team as required relating to security posture and implementation of best-practices
- Supports implementation of security principles through technical solutions, including pre-and-post-implementation testing

As a role model and champion you will work to identify and integrate safe, best practices into daily activities to foster the delivery of safe and exemplary care.

The responsibilities described above are representative and are not to be construed as all-inclusive.

EMPLOYMENT OPPORTUNITY

Qualifications/Skills:

- Bachelor Degree in Computer Science, Information Technology, Information Management, or other related field, or equivalent experience and industry certifications, such as CCNP/CCIE, CISSP, HP Ace, etc.
- 5 years in an Information Security-related role/profession
- 5 years of hands-on network or infrastructure-related technical experience
- Experience with penetration testing, vulnerability scanning and threat-risk assessments (assessment and remediation)
- Knowledge of IT security products and current threat landscape
- Strong knowledge of networking concepts, particularly next-generation firewalls
- Knowledge of IT security frameworks (COBIT, TOGAF, NIST, ISO 27001, etc.)
- Ability to document and plan multi-phase initiatives, adapting in-flight, with minimal disruption
- Familiarity with PHIPA and PIPEDA an asset
- Experience working with Cloud technologies an asset
- Should have functional knowledge of High Availability and Disaster Recovery solutions
- Good work and attendance record required.
- Strong problem solving and conflict resolution skills.
- Strong customer service skills.
- Strong analytical skills; ability to forecast comprehensive multi-year plans.
- Strong organizational skills and the ability to oversee several projects with competing priorities.
- Strong ability to produce high quality reports and meet deadlines.
- Self-starter, with strong ability to self-manage or self-direct.
- Strong interpersonal skills in order to interact with individuals in a wide range of situations.
- Strong verbal and written communication skills.
- Strong critical thinking, judgement and analysis.
- Professional behavior and communication that meets the standards of the professional regulatory college or association, as applicable, and the standards of Women's College Hospital
- This position plays a critical role in acting as an advocate for safety and will demonstrate principles, practices and processes that will optimize a safe environment for all

POSTING DATE: July 18, 2018

Please forward resumes via email to HR@wchospital.ca with your name and the competition number in the subject line. (Example: Jane Smith, 1.16)

We thank you for your interest, however, only qualified applicants who are selected to be interviewed will be contacted.

Women's College Hospital is a fully affiliated teaching hospital of the University of Toronto and is committed to fairness and equity in employment and our recruitment and selection practices. We encourage applications from Indigenous peoples, people with disabilities, members of sexual minority groups, members of racialized groups, women and any others who may contribute to the further diversification of our Hospital community. Accommodation will be provided in all parts of the hiring process as required under our Access for People with Disabilities policy. Applicants need to make their requirements known in advance.