Job Title: Digital Senior Security Advisor

At the Region of Halton, we treat everyone with respect, honesty, fairness and trust. As an equal opportunity employer, we are committed to establishing a qualified workforce that is reflective of the diverse population we serve. The Region of Halton is committed to providing accommodations throughout the recruitment process.

Halton Region serves more than 595,000 residents throughout Burlington, Halton Hills, Milton and Oakville. We are committed to delivering high quality programs and services that make Halton a great place to live and work.

Joining Halton Region opens the door to a fulfilling career. Our comprehensive compensation, great benefits and employee recognition program are a few reasons why we are one of the GTA's Top Employers.

We engage great people who contribute to meaningful work that makes a positive difference in our community. As an employee, you will be part of a progressive, service focused and award winning employer with a diverse and inclusive work environment. At Halton, you are encouraged to grow and succeed in your career and are recognized for your accomplishments and contributions.

Posting ID: 526
Department: Digital & Information Services
Job Type: Permanent
Hours of Work: 35 hours per week
Work Location: Halton Regional Centre - 1151 Bronte Road, Oakville
Employee Group: MMSG
Posting Date: April 1, 2022
Application Deadline: Until Fulfilled

Job Summary

Reporting to the Director, Digital Workplace and Technology, this position will be responsible for the development and delivery of a comprehensive organizational information security program. This position will oversee and manage digital technology and digital information management security programs across the Region. The successful candidate will collaborate to identify, develop, and implement cyber security initiatives, policies, standards, and procedures related to information technology and information management and is accountable for ongoing monitoring, compliance, and improvement and enhancement.

Duties & Responsibilities

- Leads the implementation of the Region's cyber security program, the development and implementation of digital information technology and digital information management cyber security policies, standards, and procedures.
- Leads the development and delivery of awareness and training concerning information security, which includes developing strategic and tactical plans, implementing the various means of heightening awareness, monitoring, and evaluating and revising or developing alternative or additional approaches.
- Leads the development and implementation of the Region's cyber incident response program.
- Develop and implement an ongoing risk assessment program targeting digital information security and privacy matters; recommend methods for vulnerability detection and remediation, and oversee vulnerability testing.
- Develops and maintains the processes involved in managing risks. Regularly facilitates reviews to assess the state of identified risk; develops preventative measures to mitigate risk.
- Responsible for addressing compliance and risk management, reporting to the Region's senior management on the state of compliance, potential risks, and mitigation strategy.
- Performs vulnerability assessment of digital systems using industry best practices.
- Ensures the enforcement of digital security policies across the Region, including Information Technology.
- Ensures security of enterprise information systems by evaluating Regional and IT strategies and requirements, analyzing vulnerabilities and risk, planning, and implementation of strategic initiatives.
- Evaluates the Digital and Regional strategic plans and ensure that security technology/information management protocols are defined and applied.
- Provides Digital Information Services and Regional departments/divisions with security-related consulting services on technology and information management and offers insights or advice on best industry

practices.
- Works in collaboration with IT and other Regional staff identifies and implements approved tools and resources to monitor the use of technology and identify technology and/or information-related security breaches or misuse.
- Serves as an active member of security-related industry workgroups/committees.
- Contributes subject matter advice and recommendations on the Region's Disaster Recovery Plan (DRP).
- Performs other duties as assigned.

Skills & Qualifications

Essential

- Bachelor’s degree in Computer Science, Information Technology or a related discipline or equivalent experience with five (5) years of experience managing enterprise-class infrastructure in a multi/hybrid Cloud environment that includes Azure (inclusive of Office365), AWS, and on-premise, and Cloud.
- Three (3) to five (5) years experience working in IT management.
- Experience with modern Cloud infrastructure, network monitoring and management tools, NIST Framework, ITIL, complex networks.
- Knowledge of current information security, audit and legal industry practices and standards, specifically *ISO 17799, NIST, COBIT, PIPEDA, PHIPA and ITIL* are required along with strong knowledge of LAN/WAN configuration and design, VPN, firewalls, wireless, Windows Active Directory and TCP/IP.
- Understanding of information security principles and best practice (e.g., *ISO27001 and ISF Standards of Good Practice for Information Security*).
- Excellent oral written and presentation skills are necessary along with strong interpersonal skills and the ability to work in a team environment.
- The ability to prioritize, communicate and organize multiple projects of varying complexity, frequently under deadline pressure.
- Experience with Building Automation Systems, SIEM, MDR, Security tools for network and endpoint security, Firewalls (Fortinet, Palo Alto,), Citrix, and WVD/Workspaces.

Preferred

- Industry qualifications - *CISSP / CISA / CRISC / SABSA*.

Working/ Employment Conditions

Employment Conditions

- Current (obtained within the past six (6) months), original and acceptable Criminal Records Check by the first day of employment.
- In support of the Region’s commitment to a healthy and safe workplace and community, the Region has a vaccination requirement for all employees. The successful candidate will be made an offer of employment on the condition of being fully vaccinated against COVID-19 and able to provide proof of vaccination. The candidate will be asked to provide the Region with proof of full vaccination, prior to their employment start date. The requirement to be fully vaccinated is subject to the Ontario Human Rights Code. If the candidate is unable to vaccinate for a reason protected by the Code, a request for accommodation can be requested and written proof satisfactory to the Region will be required.

Important information about your application:

- If you require accommodation, please notify us and we will work with you to meet your needs.
- We encourage applications from all qualified individuals; however, only those under consideration will be contacted.
- Applications will be accepted up to midnight of the application deadline.
- If you experience any issues with submitting your application, please contact HR Access at 905-825-6000 extension 7700.
- Applications that are not submitted online will not be considered.
- Personal information collected through the job application process will only be used for the purpose of determining qualifications for employment.
- If selected for an interview, you will be contacted by email and/or phone. Please ensure the contact information provided on your resume is up to date and that you check your email and voicemail regularly.