Job Title:	Associate Director, Chief Information Security Officer		
Job Opening Id:	42811	**# Required:**	1
Business Unit:	Corporate Services	**Division:**	I.T. Solutions
Location:	Thorold, ON	**Standard Hours:**	35.00 / week
Full/Part Time:	Full-Time	**Regular/Temporary**:	Regular
Salary Grade:	8	**Salary Range:**	$133,450.00 - $157,000.00
Post Date:	2025-06-24	**Close Date:**	2025-07-14

SALARY CURRENTLY UNDER REVIEW

This position currently falls within our hybrid model.

About Us

Serving a diverse urban and rural population of more than 475,000, Niagara Region is focused on building a strong and prosperous Niagara. Working collaboratively with 12 local area municipalities and numerous community partners, the Region delivers a range of high-quality programs and services to support and advance the well-being of individuals, families and communities within its boundaries. Nestled between the great lakes of Erie and Ontario, the Niagara peninsula features some of Canada's most fertile agricultural land, the majesty of Niagara Falls and communities that are rich in both history and recreational and cultural opportunities. Niagara boasts dynamic modern cities, Canada's most developed wine industry, a temperate climate, extraordinary theatre, and some of Ontario's most breathtaking countryside. An international destination with easy access to its binational U.S. neighbour New York State, Niagara attracts over 14 million visitors annually, as well as a steady stream of new residents and businesses.

At Niagara Region, we value diversity - in background and experience. We are proud to be an equal opportunity employer. We aspire to hire and grow a workforce reflective of the diverse community we serve. By doing so, we can deliver better programs and services across Niagara.
We welcome all applicants! For more information about diversity, equity, and inclusion at Niagara Region, *Diversity, Equity and Inclusion - Niagara Region, Ontario* or email related questions to diversity@niagararegion.ca. To send input on reducing barriers in the current hiring process, please email myhr@niagararegion.ca. For the Region's full employee equity statement, Working at Niagara Region - Niagara Region, Ontario.

Job Summary

Salary Pending Review

Reporting to the Chief Information Officer, the Associate Director, Chief Information Security Officer (CISO) is responsible for setting the strategic direction and overseeing the development and continuous support of an enterprise-wide information security program. This role leads the planning and implementation of IT systems designed to safeguard business operations and facility defenses against security breaches and vulnerabilities. The CISO is focused on strategically anticipating, assessing, and managing emerging security threats that could impact the organization, while collaborating with senior leadership to align security initiatives with broader business goals. Additionally, the CISO develops solutions to mitigate risks and ensures the effective administration of security policies, activities, and standards, including auditing existing systems for compliance and effectiveness.

Education

- Bachelor's degree in Information Technology, Computer Science, related discipline or equivalent combination of education and experience may be considered.

Knowledge

- Minimum 10 years of progressively senior level experience in IT management, facilitation and strategic planning related to Cyber Security, Threat Risk Analysis, and Information Management in a medium to large organization of complex diverse nature.
- Proven experience in strategic planning, information systems security design, network design, disaster recovery planning, policy development, organizational change, emergency response management and client support services.
- Demonstrated ability to apply IT in solving business problems.
- Experience with systems design and development from business requirements analysis through to day-to-day management.
- Excellent understanding of project management principles - PMP designation is preferred.
- In-depth knowledge of applicable laws and regulations as they relate to information security.
- Knowledge and understanding of the Personal Health Information Protection Act (PHIPA) and Municipal Freedom of Information and Protection of Privacy Act (MFIPPA) and how these apply to the collection, storage, use and retention of data.
- Security related certification required, such as CISSP, CISM, CISO, or CISA.
- Knowledge of regulatory and industry standards such as ISO, NIST, COBIT, GDPR and other security frameworks.
- Understanding of information systems and networks and all areas of Information Security including data protection, incident management, and vulnerability management.
- Knowledge of development and management of business continuity and disaster recovery planning.
- Previous experience with IT systems threat/risk assessments, IT audits and regulatory compliance such as SOX and GDPR would be an asset.
- Experience with cloud security controls and administration would be an asset.

Responsibilities

Provides leadership and direction in the development and execution of service delivery programs and initiatives that support cyber security defense, risk management and information technology audits, to support and enable the alignment and achievement of strategic goals at the division, department, and corporate level. (40% of time)

- Leads the overall vision and strategic direction of the cyber security programs and initiatives.
- Provides leadership to the department in managing all operational aspects of the cyber security portfolio, establishing goals and objectives that align with the divisional operations plan and strategic directions, Departmental and Corporate priorities, and the Council Business Plan.
- Develops, implements, and oversees the administration of IT security policies, procedures, and standards to ensure the protection of the organization's information systems and data.
- Develops and executes short and long-term plans and measures and evaluates progress accordingly.
- Oversees the enterprise's security architecture design and security awareness training program, and offers strategic guidance for security initiatives and advancements across all corporate divisions.
- Oversees the design and execution of vulnerability assessments, penetration tests and security audits.
- Oversees the administration of all computer security systems and their corresponding or associated software, including firewalls, intrusion detection systems, cryptography systems, and anti-virus software to ensure activities are efficient and effective, identifying opportunities for streamlining processes while ensuring the most effective use of technology.
- Prepares specifications for, evaluates, and recommends approvals for technology equipment and systems offered on bids, RFP's, etc as well as negotiating contracts with suppliers and agencies.
- Oversees the acquisition, deployment, integration and initial configuration of all new security solutions or enhancements to existing security solutions.
- Provides consultation to the Corporate Leadership Team (CLT) on the design and implementation of disaster recovery and business continuity plans, procedures, audits, and enhancements.
- Maintains up-to-date knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors.
- Conducts research to further policy development, identify best practices and advance innovative solutions.

Oversees the development and implementation of the corporate-wide Information Security Governance program and strategies ensuring alignment with the Information Technology Program and Corporate Enterprise Information Program and ensuring legislative compliance. Acts as the technology lead for the Security Governance Steering Committee and builds and maintains effective partnerships with all Regional departments, shared service partners, external agencies, and tier of government. (25% of time)

- Executes departmental strategies that support the implementation of the corporate wide information security governance program, ensuring alignment with Council's strategies priorities and CLT goals and objectives.
- Promotes awareness and understanding of the important of information security among staff at the Niagara Region and its shared services partners.
- Implements change-management programs, facilitating activities and conducting interventions as required.
- Provides strategic input and contributions to the development of the overall Information Technology Program.
- Ensure that security governance policies, procedures, and controls are aligned with the organization's overall Information Technology Program and Corporate Enterprise Information Program.
- Leads the continuous evaluation and improvement of the corporate-wide Information Security Governance program, ensuring it adapts to emerging risks, technological advancements, and changes in legislative requirements.

- Works collaboratively with other Regional Departments, Divisions, and Agencies to deliver an integrated cross-departmental Cyber Security program. Oversees the development and maintenance of the IT security strategy, governance, management, and architecture, ensuring goals and objectives of the Information Technology and Enterprise Information programs are incorporated.
- Develops and manages relationships with external partners and vendors.
- Develops and maintains effective working relationships and communications with assigned departments, ABC's, area municipalities, the province and shared service partners to build consensus, resolve issues and complaints and ensure business needs are addressed.
- Collaborates with CIO, Privacy Officer, and HR to establish and maintain a system for ensuring that security and privacy policies are met.

Provide leadership, direction, and accountability during cybersecurity incidents, serving, in conjunction with the CIO, as the primary decision-maker and escalation point for incident response efforts across the organization. (5% of time

Build and maintain relationships with internal and external stakeholders to foster consensus and partnerships, ensure effective management of shared services, and collaborate with other levels of government, boards, and agencies (10% of time).

- Builds and fosters trust with clients, stakeholders, and partners alike.
- Represents Niagara Region at various user conferences and meetings, participating in working groups to ensure corporate policies and cyber security programs remain current.
- Generates, pursues, and promotes opportunities to offer viable services under a shared services model to Regional agencies, boards, and commissions and local area municipalities, participating in the negotiation, execution, and review of Service Level Agreements and/or one-time Service Contracts for provision of related shared services.
- Identifies, investigates, and facilitates relationships with cyber security research groups and various levels of government for the purposes of writing grant proposals and pursuing funds as well as developing strategic partnerships.
- Coordinates and leads collaboration meetings with Area Municipalities when necessary. Attend area municipal Council/Committee meetings and other public meetings as required.
- Member of the IT Solutions Management team, assessing, developing, and implementing activities that align with the broader organizational priorities
- Prepares reports and presentations on proceedings for Regional Council and Corporate Services Committee and Corporate Leadership Team, as required.

Manages people resource planning for the division or operating unit, determining ideal organizational structures, identifying desirable role and skill mix requirements, and ensuring ongoing work quality and deliverability of results. (10% of time)

- Enables results with the organization's human capital strategy to foster employee engagement.
- Directs and provides leadership for the activities and coaching of direct reports, providing work direction, setting priorities, assigning tasks/projects, determining methods and procedures to be used, resolving problems, ensuring results are achieved, and managing staff recruitment, performance, and skill development activities
- Ensures alignment and coordination of activity and quality of output between teams under their direction
- Ensures focus is service excellence, communication/transparency, innovation, and data integrity and workflow integration.
- Ensures staff has the information and resources to make successful plans and decisions.

- Ensures all people related issues, including recruitment, grievances, and labour relations issues, are aligned to HR and Corporate standards and practices.
- Helps to break down barriers to employee success, ensuring collaboration and cooperation with other teams within their division and department
- Ensures Occupational Health & Safety policies, programs and practices are implemented, and maintained. This includes workplace inspections, monitoring, accident reporting and investigations, and ensuring any observed hazards or lapses in the functioning of OH&S processes, and other OH&S concerns are responded to promptly.
- Ensures all individuals under supervision have been informed of hazards and instructed on the necessary risk control and emergency response measures.

Develops, manages, and administers annual and multi-year Capital and Operating budgets for the operating unit ensuring support of Council's objectives, financial transparency and accountability, monitoring budget adherence, identifying and explaining variances, and financial reporting is effectively managed in compliance with corporate financial policies. Ensure goods and services are acquired in accordance with the procurement policy. Authorize, and administer the acquisition of goods and services for the operating unit and direct reports in accordance with the procurement policy and procedures. (10% of time)

Perform other related duties and responsibilities as assigned or required.

Special Requirements

- In accordance with the Corporate Criminal Record Check Policy, the position requires the incumbent to undergo a Criminal Records Check and submit a Canadian Police Clearance Certificate.
- Must maintain ability to travel in a timely manner to other offices, work locations or sites as authorized by the Corporation for business reasons.
- May be required to support emergency operations under the incident management structure, at the direction of the Emergency Operations Centre Director.
- Regional staff strive to enable the strategic priorities of council and the organization through the completion of their work. Staff carry out their work by demonstrating the corporate values.

How to Apply

Regional staff strive to enable the strategic priorities of council and the organization through the completion of their work. Staff carry out their work by demonstrating the corporate values. To view the full job description, requirements and apply on our Careers Site, visit our Careers page - Job Opening **#42811** (https://www.niagararegion.ca/government/hr/careers/)

Uncover the wonder of the Niagara Region and join a team dedicated to meeting tomorrow's challenges, today!

Let us know why you would be an excellent team member by submitting your online application no later than **July 14, 2025,** before midnight by visiting our 'Careers' page at www.niagararegion.ca. We thank all candidates for their interest however, only those candidates selected for an interview will be contacted.