THE CORPORATION OF THE TOWN OF OAKVILLE

JOB POSTING

POSITION ID: 1591-001 CALL NO. 26-4650

Job Designation:	Senior Security Architect
Department:	Information Technology Solutions
Job Details:	Permanent, Full Time (Non-Union)
Salary Range:	$120,246 to $144,353
Pay Grade:	207
Closing Date:	Applications for this position must be received at oakville.ca no later than 11:59pm on **July 2, 2026.**
Posting Status:	Open to all current Town of Oakville employees and external applicants.

We offer:

- A hybrid work schedule
- A defined benefit pension plan (OMERS)
- Comprehensive health plan complemented with life and disability insurance
- A progressive work environment that promotes a work/life balance and strives to be a great place for great people to do great things

This job posting is for an existing vacancy and therefore will be filled accordingly.

Reporting to the Information Security Officer & Program Manager, the Senior Security Architect provides senior-level expertise in the design, implementation, and governance of security architecture across the enterprise with an emphasis on protecting sensitive data, securing cloud platforms and workloads, and leading incident response (IR) execution and maturity. This role partners closely with application, infrastructure, risk/compliance, and business leaders to reduce security risk while enabling delivery speed and operational resilience.

What can I expect to do in this role?

Data Security

- Maintain and design the evolution of enterprise data security architecture, including verifying data classification, labeling, and handling standards.
- Define and govern controls for data-in-transit and data-at-rest encryption, key management, secrets management, and certificate strategy.
- Architect and implement data loss prevention (DLP) and data egress controls across endpoints, email/collaboration, SaaS, and cloud platforms.
- Establish secure access models, including least privilege and privileged access controls for data platforms.
- Design privileged access and least privileged patterns for data platforms (e.g., data warehouses/lakes, analytics platforms) including break-glass access and approval workflows.
- Develop reference architectures for tokenization, masking, anonymization/pseudonymization, and privacy-by-design patterns aligned to regulatory requirements.
- Embed secure data lifecycle controls (collection, processing, sharing retention, archival, disposal) across systems in collaboration with data management, records management, and application teams.
- Establish security requirements and review designs for new data use cases (APIs, integrations, analytics, AI/ML), focusing on lineage, access boundaries and misuse resistance.
- Lead security risk assessments of data-centric systems and third parties; drive remediation planning and execution.
- Provides architecture guidance and guardrails that enable teams to execute quickly while meeting data protection obligations.
- Define and enforce secure data access patterns for AI-enabled solutions, with a focus on tenant data isolation
- Design controls to prevent data leakage and cross-tenant exposure in systems leveraging generative or agentic AI

- Evaluate how AI-driven workflows interact with sensitive data and ensure alignment with enterprise data protection standards

Cloud Security & Infrastructure

- Define security architecture patterns across cloud and on-premises environments, including identity, network segmentation, workload isolation and secure service-to-service communication.
- Partners with infrastructure and application teams to implement baseline cloud controls including policy-as-code, secure landing zones, and standardized account/subscription structure.
- Architect cloud identity and access management (IAM) strategies, including federation, control access, RBAC, and privileged identity workflows.
- Design secure CI/CD and infrastructure-as-code pipelines with integrated security controls.
- Establishes cloud threat modeling and secure design review practices for new services and significant changes.
- Drive cloud security posture management (CSPM) and vulnerability management, by defining remediation standards, exceptions and engineering playbooks.
- Ensure security, resiliency, and compliance requirements are built into cloud services (backup, recovery, encryption, key rotation and logging).
- Defines future state security architecture and continuous improvements
- Integrate emerging AI capabilities (e.g., agentic workflows) into cloud security architectures in a secure and scalable manner
- Design and review identity and access models supporting AI services, including delegated permissions and service-to-service trust

Incident Response Leadership

- Serve as a senior technical authority during security incidents, guiding response strategies and risk-based decisions.
- Lead development and continuous improvement of incident response playbooks for key scenarios (e.g., data breaches, ransomware, account compromise).
- Coordinate with SOC, IT, and engineering teams to define incident severity criteria, escalation paths, and communication cadences
- Lead post-incident reviews (PIRs) and ensure effective remediation of root causes.
- Translate incident learnings into improved security architecture (controls, detections, segmentation, identity hardening, data protections).
- Plan and execute tabletop exercises and simulations to enhance organizational readiness and improve cross-functional coordination.
- Advise on forensic readiness, logging, and evidence collection practices to support investigations and legal/regulatory needs.
- Participate in on-call or incident commander rotations as needed.
- Assess and prepare for security risks introduced by AI systems, including misuse of AI agents and unintended actions
- Provide guidance on detecting and responding to incidents involving AI-driven access or data exposure
- Support development of playbooks and response strategies for emerging threats related to agentic or autonomous systems

How do I qualify?

- Completion of a minimum three-year Diploma or Bachelor's Degree in Business Administration, Computer Science, Information Systems, or a related field.
- Certifications in CISSP, CISM, CISA, CCIE plus relevant cloud security certifications from Microsoft or AWS.
- Master’s degree in Cybersecurity would be considered an asset.
- Minimum 8 years of progressive information security experience, including hands-on security architecture for enterprise environments.
- Deep expertise in data security concepts and controls (classification, DLP, encryption, key management, access governance, data lifecycle).
- Experience using Microsoft Purview.
- Strong cloud security experience in at least one major cloud provider (e.g., Azure, AWS, GCP), including IAM and platform guardrails.
- Demonstrated incident response leadership experience (technical lead/incident commander role) and familiarity with common IR frameworks and practices.
- Ability to create clear security requirements and infrastructure teams through consultation and governance.
- Proficiency in threat modeling, risk assessment, and translating risk into actionable engineering work.
- Strong written and verbal communication skills, including the ability to explain complex security trade-offs to technical and non-technical stakeholders.

Please note that this position requires a satisfactory criminal record check dated within the last 30 days as a condition of employment.

Core Knowledge Required for Success
In addition, your experience demonstrates the following:

- **Strategic Thinking** – thinking things through
- **Engagement** – working effectively with people, organizations and partners
- **Management excellence** – delivering results through own work, relationships and responsibilities
- **Accountability and Respect** – serving with integrity and respect

Corporate Values:
Teamwork, accountability, dedication, honesty, innovation and respect

DATED: June 19, 2026

The Town's recruitment software includes elements of artificial intelligence to assist in the screening and short-listing of qualified candidates.

This job profile reflects the general requirements necessary to perform the principal functions of the job. This does not include all of the work requirements of the job. Applicants are required to demonstrate through their application and in the interview process that their qualifications match those specified. Applicants may also be required to undergo testing.

We thank all applicants and advise that only those selected for an interview will be contacted.