



THE CORPORATION OF THE TOWN OF OAKVILLE

JOB POSTING

POSITION ID: 1591-001

CALL NO. 26-4729

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 September 13, 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.

What can I expect to do in this role?

Security Architecture & Solution Design

- Lead security architecture reviews for major projects and technology initiatives.
- Develop security reference architectures, standards, patterns and design guidance.
- Review application, infrastructure, cloud and integration designs and provide security recommendations.
- Partner with technical teams to incorporate security requirements into solution designs.
- Serve as the Town's subject matter expert for enterprise security architecture.

Data Security

- Define and maintain enterprise data security architecture, standards, and controls to protect sensitive information throughout its lifecycle.
- Establish security requirements and architecture patterns for data classification, encryption, key management, secrets management, and privacy protection.
- Design and implement data protection capabilities including data loss prevention (DLP), data access governance, and data egress controls across on-premises and cloud environments.
- Develop secure access models and privileged access controls for enterprise data platforms, applications, analytics solutions, and integrations.
- Establish reference architectures and security patterns for data sharing, analytics, AI-enabled solutions, and emerging technologies.
- Partner with business and technology teams to embed security controls and privacy requirements into data-related initiatives and services.
- Lead security reviews and risk assessments of data-centric systems, technologies, and third-party solutions, and drive remediation activities.
- Define and enforce secure data access and protection controls for AI-enabled solutions, with a focus on tenant isolation, data leakage prevention, and regulatory compliance.

Cloud Security & Infrastructure

- Define and maintain enterprise security architecture, standards, and controls across cloud and on-premises environments.
- Establish architecture patterns for identity and access management (IAM), network security, workload isolation, and secure service-to-service communications.

Successful candidates will abide by Ontario Health & Safety Legislation and follow Corporate Health & Safety Policies.

The Town of Oakville is an equal opportunity employer.

Personal information collected from applications and resumes is collected under the authority of the *Municipal Act, 2001*, and will be used to determine qualifications for employment. Questions about this collection of information should be directed to Human Resource Services, 1225 Trafalgar Road, Oakville, Ontario L6H 0H3.

- Design and implement secure cloud foundations, including landing zones, policy-as-code, infrastructure-as-code, and secure CI/CD pipelines.
- Develop and govern cloud access control models, including federation, role-based access control (RBAC), privileged access management, and delegated administration.
- Establish threat modelling and security design review practices for cloud services, applications, and technology initiatives.
- Lead cloud security posture management (CSPM), vulnerability management, and remediation initiatives by defining standards, processes, and technical guidance.
- Ensure security, resiliency, and compliance requirements are incorporated into cloud services, including encryption, logging, monitoring, backup, recovery, and key management.
- Develop reference architectures and security patterns for emerging technologies, including AI-enabled and agentic solutions.
- Partner with technology teams to continuously improve enterprise security capabilities, architecture standards, and operational resilience.

Incident Response Leadership

- Provide senior technical expertise and architectural guidance during cybersecurity incidents.
- Develop and maintain incident response playbooks, procedures, and readiness exercises.
- Lead post-incident reviews and drive security improvements based on lessons learned.
- Support forensic readiness and response planning for emerging threats, including AI-related security incidents

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.

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: [August 28, 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.

Successful candidates will abide by Ontario Health & Safety Legislation and follow Corporate Health & Safety Policies.

The Town of Oakville is an equal opportunity employer.

Personal information collected from applications and resumes is collected under the authority of the *Municipal Act, 2001*, and will be used to determine qualifications for employment. Questions about this collection of information should be directed to Human Resource Services, 1225 Trafalgar Road, Oakville, Ontario L6H 0H3.