Elections Ontario

Director, Cybersecurity and IT Risk

Position Status:	Permanent
Posting Status:	Open
Location:	(On-site) 26 Prince Andrew Place, Toronto, Ontario M3C 2H4 (Don Mills and Eglinton)
Starting Salary:	$160,317 – $201,962 per year
Hours of Work:	36.25 per week
Posting Date:	August 18, 2026
Closing Date:	September 18, 2026

Who are we

The Office of the Chief Electoral Officer (Elections Ontario) is an independent, non-partisan office of the Legislative Assembly of Ontario, responsible for administering provincial elections, by-elections, and referenda in Ontario. We are committed to making voting easy and accessible for all electors, while maintaining the integrity, security, and transparency of the electoral process.

Join our team

The Information Technology and Register Services (ITRS) Cluster of Elections Ontario is seeking a highly motivated and innovative leader to set the strategic direction for cybersecurity and IT risk, provide trusted advice to senior leaders, and translate complex security issues into clear risks, options, and recommendations.

The incumbent will oversee cybersecurity governance, risk management, compliance, security operations, incident response, and election readiness activities, with a strong focus on safeguarding critical systems, sensitive information, and public trust.

What to expect in this role

Reporting to the Chief Information Officer, you will:

Play a critical leadership role in protecting the systems, data, and technology that support Ontario's electoral process. You will lead the development and delivery of Elections Ontario's cybersecurity and IT risk program, ensuring the organization is prepared to identify, manage, and respond to evolving cyber threats.

You will lead and support a team of cybersecurity professionals, establish priorities, manage resources, and ensure the team is equipped to deliver effective services during regular operations and periods of heightened election readiness. You will also work

Elections Ontario

closely with internal teams, vendors, public-sector partners, and other electoral agencies to strengthen resilience, coordinate responses, and support continuous improvement.

Key responsibilities will include:

- Developing and operationalizing a multi-year cybersecurity and IT risk strategy aligned with organizational priorities and election readiness needs.
- Advising the CIO and senior leaders on cyber risk posture, emerging threats, investment priorities, and mitigation strategies.
- Leading cybersecurity governance, risk frameworks, policies, standards, procedures, and compliance activities.
- Overseeing security operations, including threat monitoring, detection, escalation, response, recovery, and post-incident review.
- Acting as a senior lead during significant cybersecurity incidents and coordinating response activities across internal teams, vendors, and external partners.
- Leading cyber and IT risk assessments, mitigation planning, monitoring, and reporting using recognized frameworks such as NIST, ISO, and CIS.
- Ensuring cybersecurity practices support legislative, privacy, and data protection requirements related to electoral and financial information.
- Planning and leading cybersecurity readiness activities for election events, including testing, simulations, threat risk assessments, and continuity planning.
- Providing cybersecurity oversight for technology initiatives, cloud services, applications, infrastructure, and identity and access management.
- Managing cybersecurity projects, procurement activities, vendor relationships, contracts, budgets, and resources.
- Building strong relationships across Elections Ontario, government, industry, vendors, and other electoral agencies to support coordination, knowledge sharing, and resilience.

What you need to qualify

- Demonstrated progressively responsible experience in cybersecurity, IT security, IT risk, or a related field, including leadership experience managing teams, programs, priorities, and resources.
- Demonstrated experience developing and delivering cybersecurity strategies, roadmaps, governance models, and large-scale security initiatives.
- Strong knowledge of cybersecurity governance, risk management, compliance, and recognized frameworks such as NIST, ISO/IEC 27001, CIS Controls, COBIT, or related methodologies.
- Experience overseeing cybersecurity operations, including threat and vulnerability management, security monitoring, incident response, escalation protocols, and recovery activities.

Elections Ontario

- Knowledge of secure technology architecture and controls across infrastructure, cloud services, applications, identity and access management, and data protection.
- Experience translating complex cybersecurity and IT risk issues into clear advice, recommendations, and decision-support materials for senior leaders and non-technical audiences.
- Demonstrated experience developing and governing AI security and risk management frameworks that enable responsible innovation while safeguarding sensitive information, maintaining public trust, and protecting election integrity
- Knowledge of applicable legislation, privacy obligations, confidentiality requirements, and regulatory expectations related to protecting sensitive information.
- Experience with business continuity, disaster recovery, resilience planning, penetration testing, threat risk assessments, and simulation exercises.
- Experience managing cybersecurity vendors, contracts, procurements, service performance, budgets, and resources.
- Experience in the public sector, a highly regulated environment, critical infrastructure, or high-profile operational setting is considered an asset.
- Professional cybersecurity or risk certifications such as CISSP, CISM, CRISC, CISA, or an equivalent certification are considered assets.
- Highly developed interpersonal, communication, relationship management and partnership building skills.
- Highly developed project, budget and financial management skills and experience.
- Demonstrated analytical, problem solving and organizational skills.
- Must be legally entitled to work in Canada.

This position requires in-office presence of five days per week. There is no hybrid opportunity.

The successful candidate will be required to complete criminal background and social media checks as part of the recruitment process.

Elections Ontario

How to apply

Our recruitment process reflects our mission to uphold the integrity and accessibility of the electoral process and to manage elections in an efficient, fair, and impartial manner. We offer career growth opportunities and a competitive rewards program.

Please submit your cover letter and resume as one attachment, quoting File **#EO-2026-104** First Name Last Name in the subject line, to jobs@elections.on.ca no later than **4PM on September 18, 2026.**

We thank all applicants for their submission. Only those candidates selected for an interview will be contacted.

How to request an accommodation

Elections Ontario is an equal opportunity employer. We are committed to fostering an inclusive, equitable and accessible environment, where all employees feel valued, respected, and supported.

Under the *Accessibility for Ontarians with Disabilities Act* and the *Ontario Human Rights Code*, we provide accommodations to applicants with disabilities throughout the recruitment and selection process. If you require a disability-related accommodation to participate, please call 1-888-668-8683, send a fax to 1-866-714-2809, TTY at 1-888-292-2312 or email hr@elections.on.ca.

At Elections Ontario, all resumes are screened by the Talent Acquisition team and Hiring Managers, without the use of AI. Criminal record checks also do not use AI. However, AI technology is used when conducting social media checks.

Elections Ontario posts salaries in accordance with ESA pay/transparency legislation. Individual salaries within the anticipated salary range are determined through various factors, including but not limited to internal equity, education, relevant experience, knowledge and applicable skill sets.