



Contribute to the City of Hamilton, one of Canada's largest cities - home to a diverse and strong economy, an active and inclusive community, a robust cultural and dining scene, hundreds of kilometers of hiking trails and natural beauty just minutes from the downtown core, and so much more. Join our diverse team of talented and ambitious staff who embody our values of sensational service, courageous change, steadfast integrity, collective ownership and being engaged empowered employees. Help us achieve our vision of being the best place to raise a child and age successfully. #BeTheReason

- **Job ID #32295: Manager, Cybersecurity**
- **Union:** Non-Union
- **Job Description ID #: A16006**
- **Close date:** Interested applicants please submit your application online at www.hamilton.ca/city-council/jobs-city by 4:00 p.m. on November 11, 2026.
- **Vacancy type:** This posting is for a new vacancy
- **Internal applicants should apply with your work e-mail address.** External applicants are considered only after the internal posting process has been completed. Only applicants chosen for an interview will be contacted.

SUMMARY OF DUTIES

Reporting to the CISO (Chief Information Security Officer), the Manager, Cybersecurity provides strategic and operational leadership for the City's cybersecurity program, protecting the confidentiality, integrity and availability of information and technology services.

The Manager leads assigned security professionals and service providers in security governance, risk management, threat detection, incident response, vulnerability management and security assurance across on-premises, cloud and hybrid environments.

GENERAL DUTIES

STRATEGY & PLANNING

- Leads and provides strategic direction for cybersecurity, establishing priorities, standards and operating plans aligned with corporate objectives, risk and available resources.
- Participates in IT planning and advise the CISO and IT Management Team on security risks, control effectiveness, investment priorities and decisions requiring executive direction.
- Plans security service capacity, coverage, skills and technology lifecycles to meet current and emerging needs. Allocate capacity-based services and assignments according to approved priorities, operational demand, risk and available team capability.

- Develops and communicate security policies, standards and plans. Maintain cybersecurity risk and exception records, identify accountable owners and track treatment actions; escalate residual risk for acceptance by the authorized decision-maker.
- Leads cyber incident preparedness, response playbooks and exercises. Coordinate security requirements for disaster recovery and business continuity with Infrastructure and business owners, including secure restoration, recovery testing and closure of exercise findings.
- Establishes security architecture principles and control requirements with architects and technical owners, covering identity, networks, endpoints, applications, cloud services and information protection.
- Evaluates emerging threats and security technologies, including risks arising from artificial intelligence and new digital services. Recommend proportionate controls and improvements based on business needs and evidence.
- Defines security sourcing requirements and assess supplier security risks throughout the relationship. Work with IT Operations, Procurement and Legal on RFX documents, security clauses, evaluations and service obligations; oversee security-provider performance and escalate deficiencies within delegated authority.
- Oversees security projects using approved project-management practices, ensuring defined scope, resources, testing, operational acceptance and measurable outcomes.
- Manages security operations and assigned security platforms, including monitoring, log analysis, threat detection and investigation. Oversee internal and managed security services, detection coverage, alert quality and escalation arrangements. Use threat intelligence to guide detection and response priorities; maintain current playbooks and operational documentation.
- Leads assigned security staff, including recruitment, onboarding, workload balancing, scheduling, coaching, performance management, succession and employee development. Address workplace matters in accordance with City policies and maintains a respectful, inclusive and psychologically safe workplace.
- Ensures that employees are provided with and use the appropriate equipment, material and/or procedures required to perform the assigned duties.
- Ensures that all employees perform work in accordance with applicable health and safety legislation and all City of Hamilton corporate and departmental policies and procedures. Ensures that appropriate action is recommended for those employees who do not work in compliance with legislation, policies or procedures.
- Develops and manage security operating and capital budgets, forecasts and business cases, monitoring expenditure, benefits and resource requirements.
- Maintains lifecycle, licensing and inventory accountability for assigned security tools and services in coordination with corporate asset and contract-management functions.
- Presents executive briefings, dashboards, risk recommendations and incident updates. Ensure reports and technical materials prepared by assigned specialists are accurate, timely and appropriate for their audience.
- Oversees security awareness, role-based training, phishing exercises and targeted communications through assigned staff. Evaluate effectiveness and address recurring behaviors and knowledge gaps.

ACQUISITION & DEPLOYMENT

- Improves security services through critical thinking, practical experimentation, standardization and repeatable technology-enabled practices. Provide hands-on support within the role's expertise and authority when needed to resolve complex issues or advance priority work.

OPERATIONAL MANAGEMENT

- Leads cybersecurity governance and control reviews using recognized frameworks such as NIST CSF, CIS Controls and ISO/IEC 27001, as appropriate to the City's approved program.
- Oversees identity and access security requirements, including least privilege, multifactor authentication, privileged access, access reviews and timely access removal, with the teams responsible for implementation and administration.
- Leads the coordinated response to cybersecurity incidents under the City's incident-management arrangements, including triage, investigation, containment, evidence preservation and recovery coordination. Engage the CISO, technical owners, Privacy, Legal and Communications as appropriate and track post-incident actions.
- Oversees vulnerability assessments, penetration testing and security audits. Prioritize findings by exposure, exploitability and business impact; agree remediation timelines with technical owners, validate closure and escalate overdue or accepted risks.
- Works in accordance with the provisions of applicable health and safety legislation and all City of Hamilton corporate and departmental policies and procedures related to occupational health and safety.
- Responsibilities are not exhaustive and may evolve with organizational priorities, technology, emerging risks and service demand. Perform other related duties and assigned work consistent with the position, as directed by the CISO.

QUALIFICATIONS

1. University degree in Computer Science, Information Systems, Cybersecurity or a related discipline, or an combination of equivalent education and relevant experience.
2. Extensive (preference for a minimum ten (10) years) of progressive experience in information technology or cybersecurity, including at least five (5) years in management or leadership with responsibility for security services, staff, budgets and service providers.
3. CISSP, CISM or an equivalent recognized information security certification.
4. Demonstrated experience developing cybersecurity strategies, policies, standards and operating plans aligned with organizational priorities and risk; practical knowledge of NIST CSF, CIS Controls and ISO/IEC 27001. Experience conducting security risk assessments, maintaining risk and exception records, evaluating control effectiveness and presenting treatment recommendations to authorized decision-makers.
5. Experience leading security operations and internal or managed security services, including security monitoring, log analysis, detection improvement and the use of threat intelligence to guide priorities. Experience leading cybersecurity incident response, including investigation, containment, evidence preservation, stakeholder coordination and post-incident improvement; sound judgment under pressure.

6. Experience overseeing vulnerability assessments and penetration testing, prioritizing findings by business risk, coordinating remediation with technical owners and validating closure.
7. Strong knowledge of security architecture and controls across networks, endpoints, applications and cloud and hybrid environments, including Microsoft 365 and Azure security. Understanding of operational technology and connected-device security is an asset.
8. Strong knowledge of identity and access security, including least privilege, multifactor authentication, privileged access, access reviews and account lifecycle controls.
9. Knowledge of information-protection controls, including data classification, encryption, secure handling, data-loss prevention and logging, in collaboration with data owners and Privacy.
10. Experience coordinating cyber preparedness, tabletop exercises and security requirements for business continuity and disaster recovery, including secure restoration and validation of corrective actions.
11. Knowledge of applicable cybersecurity, privacy and information-protection obligations and experience coordinating audits, evidence and corrective actions with accountable corporate functions. Municipal, public-sector or other regulated-sector experience is an asset.
12. Experience assessing supplier security risks, defining security procurement and contractual requirements, and monitoring security-provider performance throughout the service lifecycle.
13. Experience overseeing security awareness and role-based training, engaging stakeholders in behavior change and measuring program effectiveness.
14. Demonstrated people leadership, including recruitment, onboarding, coaching, performance management, workforce planning, workload balancing and succession; ability to lead collaboratively and manage change.
15. Experience developing and managing operating and capital budgets, financial forecasts, business cases and investment recommendations within delegated authority.
16. Knowledge of IT service-management and project-management practices, including incident, request, problem, change and service-level management; ability to balance operational and project demand against capacity and maintain accountable, documented work tracking.
17. Strong analytical and problem-solving skills, with the ability to challenge established approaches, assess emerging technology risks, develop practical solutions, improve recurring work through repeatable technology-enabled practices and contribute hands-on when required.
18. Excellent written and oral communication, presentation, facilitation, negotiation and conflict-resolution skills; ability to explain technical risks to nontechnical audiences, review specialist reports and provide clear executive recommendations.
19. Must possess and maintain a valid Class G Driver's Licence in the Province of Ontario.

THIS POSITION REQUIRES A VALID CLASS "G" DRIVER'S LICENCE AND PROOF THEREOF IS REQUIRED AFTER HIRE.

NOTE

The position may be required to work outside regular business hours, including evenings, weekends and statutory holidays, and to participate in on-call or emergency response arrangements during major incidents, planned maintenance, implementations, recovery exercises or service disruptions, as operationally required.

Hybrid work arrangement with approximately 50% on-site attendance, typically two (2) days one week and three (3) days the following week, subject to operational requirements. Additional on-site attendance may be required for incidents, implementations, executive meetings, critical projects, training or other operational needs.

NOTE

As a condition of employment, the successful applicant(s) will be required to obtain, satisfactory to the City of Hamilton, a Criminal Record & Judicial Matters (CRJM) Check, at their own expense, prior to beginning work in this position. The City of Hamilton will also undertake social media review of the successful candidate.

Disclaimer:

Be advised that Human Resources frequently audits resumes of internal/external applicants to ensure/validate information provided is consistent and trustworthy. Falsification of information provided at any time throughout the recruitment process may be grounds for disqualification, and for internal applicants, subject to discipline up to and including termination.

Terms:

The City is an equal opportunity employer that is committed to inclusive, barrier-free recruitment and selection processes. Consistent with our Values and Corporate Culture Pillars, the City of Hamilton is committed to providing equitable treatment to all with respect to barrier-free employment and accommodation without discrimination. The City will provide accommodation for applicants in all aspects of the hiring process, up to the point of undue hardship. If you have an accommodation need, please contact Human Resources as soon as possible to make appropriate arrangements

Location

Hamilton, Ontario (Hybrid)

Department

Corporate Services

Employment Type

Permanent, Full-Time

Minimum Experience

Manager/Supervisor

Compensation

\$127,454.60 - \$159,317.34 /annual

Internal Job Code

16006