



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 #32315: Supervisor, Cybersecurity**
- **Union:** Non-Union
- **Job Description ID #: A16009**
- **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 Manager, Cybersecurity, the Supervisor, Cybersecurity oversees day-to-day cybersecurity operations and delivery of assigned security services to protect the confidentiality, integrity and availability of the City's information and technology. The role supervises security monitoring, investigations, vulnerability management and operation of assigned security tools across on-premises, cloud and hybrid environments.

The Supervisor provides leadership, guidance and daily supervision to assigned security staff and coordinates work with service providers. Translates approved security priorities into work plans, clear assignments, effective coverage and measurable service outcomes. The Supervisor contributes security expertise to projects and works with Infrastructure, IT Operations, application teams, architects and business owners to implement controls and coordinate remediation and secure recovery. May lead security workstreams or participate in projects, escalating policy, risk and resource decisions to the Manager, Security.

GENERAL DUTIES

- Supervises the configuration, integration, maintenance and troubleshooting of assigned security platforms. Ensures monitoring coverage, reliable logging, effective alerting and timely escalation across supported environments, including services delivered by external security providers.

- Assigns and prioritizes daily security work, balancing operational demand, project commitments, risk and available team capacity. Establishes coverage and escalation arrangements and escalates resource or service gaps to the Manager.
- Implements approved security policies and control requirements. Develops and maintains operational procedures, playbooks and technical baselines with security specialists and architects; submits policy and architecture recommendations through established governance.
- Evaluates security solutions and recommends improvements to the Manager, considering control effectiveness, integration, support requirements, operational risk and cost. Supports the Manager in communicating approved security objectives, responsibilities and service priorities to staff and stakeholders.
- Contributes security design input and validates assigned controls with architects and technical owners. Documents findings, implementation requirements and exceptions for review and approval. Maintains operational risk, exception and corrective-action records; escalates unresolved or overdue issues and refers risk acceptance to the authorized decision-maker.
- Maintains assigned cyber incident and recovery procedures, coordinates tabletop exercises and supports secure-restoration testing with Infrastructure and business owners. Documents findings and follows through on corrective actions. Maintains awareness of emerging threats, attack methods and security technologies. Uses relevant threat intelligence to improve monitoring, investigation priorities and defensive measures.
- Supports security procurement by preparing technical requirements, evaluating solutions and recommending purchases or enhancements in accordance with City processes and delegated authority.
- Coordinates deployment, integration, testing and operational handover of approved security solutions and enhancements, including change approvals, rollback plans, documentation and support readiness. Coordinates implementation and verification of information-protection controls, including secure handling, encryption and data-loss prevention, with data owners, Privacy and technical teams.
- Coordinates assigned cybersecurity investigations and incident-response activities, including triage, containment, evidence preservation and recovery support under approved playbooks. Escalates significant incidents promptly, provides status updates and tracks post-incident actions.
- Coordinates vulnerability assessments, authorized penetration testing and security audits. Prioritizes findings by exposure and business impact, assigns or coordinates remediation with accountable owners, validates closure and escalates overdue actions.
- Coordinates assigned security awareness, phishing exercises and role-based training with program staff. Reviews supporting materials, tracks participation and outcomes and recommends targeted improvements.
- Conducts performance reviews, coaching and mentoring; identifies development and cross-training needs, balances workloads and supports succession planning. Addresses performance and workplace matters within delegated authority and City policies, maintaining a respectful, inclusive and psychologically safe workplace.

- Leads or participates in recruitment, interviews, assessment development and selection as delegated. Coordinates onboarding, access, training and clear performance expectations for new staff.
- Coordinates security support with Infrastructure, IT Operations, application teams and service providers. Provides hands-on investigation, troubleshooting and technical assistance within the role's expertise and authority when needed.
- Reviews, prioritizes and progresses assigned incidents, service requests, investigations and improvement actions in approved work-management systems. Personally completes assigned work, records actions and outcomes and ensures clear ownership, timely communication and closure. Maintains effective relationships with business partners and IT teams; communicates security-service impacts, planned changes and outstanding concerns through agreed channels.
- Works with security specialists, architects and technical owners to implement and validate access controls, including least privilege, multifactor authentication, privileged access, access reviews and timely access removal.
- Monitors assigned budgets and day-to-day expenditure in accordance with City policies. Prepares estimates and financial information and approves purchases only within delegated authority. Contributes to section goals, annual work plans and service targets aligned with divisional priorities and the Manager's direction.
- Acts on behalf of the Manager, Security when assigned and within delegated authority. Improves recurring security work through critical thinking, practical experimentation, standardization and repeatable technology-enabled practices. Tests and documents approved improvements and measures their effectiveness.
- Reviews operational measures for detection coverage, response, remediation, service demand and awareness. Validates specialist-prepared reports and provides concise dashboards, presentations and recommendations to the Manager and relevant stakeholders.
- Maintains inventory, licensing, ownership and lifecycle records for assigned security tools and services, coordinating with asset and contract-management functions and recommending improvements. Maintains security operational documentation and evidence, including investigation records, control checks, change records and handover materials. Supports compliance reviews and audits with accountable corporate functions and tracks assigned corrective actions.
- Monitors security-provider service levels and deliverables, coordinates supplier security reviews and escalates performance or security concerns. Works with IT Operations, Procurement and Legal on contractual matters within delegated authority.
- May be assigned to related initiatives or projects under the direction of another IT Unit Manager or Project Manager, with priorities coordinated through the Manager, Security.
- 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.

- 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. Performs other related duties and assigned work consistent with the position.

QUALIFICATIONS

1. University degree or college diploma in Computer Science, Information Systems, Cybersecurity, Computer Technology or a related discipline, or a combination of equivalent education and relevant experience.
2. One or more recognized information security certifications relevant to the role, such as CISSP, CISM or an equivalent technical or security-leadership certification.
3. Five (5) or more years of relevant cybersecurity experience, including security implementation, administration and operational support, with demonstrated previous experience in a supervisory or team-lead capacity.
4. Experience supervising security operations, monitoring, log analysis, alert triage and investigations, including coordination with managed security providers and the use of threat intelligence. Experience configuring, maintaining or supervising endpoint protection, security monitoring, intrusion detection and related security tools; ability to improve recurring work through approved, repeatable technology-enabled practices.
5. Experience coordinating cybersecurity incident response, containment, evidence preservation, stakeholder escalation and post-incident improvement under approved procedures. Experience supporting cyber preparedness, tabletop exercises and secure-recovery testing with Infrastructure and business owners, and tracking findings and corrective actions.
6. Experience coordinating vulnerability assessments, penetration testing and remediation; ability to prioritize findings by risk, work with technical owners and validate corrective actions.
7. Working knowledge of identity and access security, including multifactor authentication, privileged access, least privilege, access reviews and account lifecycle controls. Knowledge of information-protection controls, including secure handling, encryption and data-loss prevention, and the roles of data owners and Privacy.
8. Working knowledge of security controls for cloud and hybrid environments, including Microsoft 365, Azure, email and mobile devices; ability to assess configuration and access risks with technical specialists.
9. Demonstrated ability to supervise and develop staff, including scheduling, workload allocation, recruitment, onboarding, coaching, performance management and cross-training, and to maintain a respectful and inclusive workplace.
10. Strong analytical, planning and troubleshooting skills; sound judgment under pressure, ability to challenge established approaches and develop practical solutions, and willingness to contribute hands-on within assigned expertise and authority.

11. Knowledge of IT service-management practices, including incident, request, problem, change and service-level management; experience maintaining documented assignments, actions, escalations and closure records.
12. Knowledge of project-management principles and experience coordinating security workstreams, estimates, testing and handover; ability to monitor expenditure, procurement requirements and supplier deliverables within delegated authority.
13. Working knowledge of TCP/IP, DNS, authentication, network segmentation and secure connectivity sufficient to investigate security events and assess controls with network specialists. Understanding of operational technology security is an asset.
14. Knowledge of recognized cybersecurity frameworks and control practices, such as NIST CSF, CIS Controls and ISO/IEC 27001; ability to translate approved requirements into operational procedures and evidence.
15. Knowledge of applicable cybersecurity, privacy and information-protection obligations; experience supporting compliance reviews, audits and corrective actions with accountable corporate functions. Municipal, public-sector or other regulated-sector experience is an asset.
16. Strong interpersonal, written and oral communication, presentation and conflict-resolution skills; ability to explain technical issues, review specialist reports, support security awareness and training, and collaborate across teams.
17. 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.

THE INCUMBENT SHALL COMPLY WITH ALL HEALTH AND SAFETY POLICIES AND PRACTICES FOR THIS POSITION AND THE WORKPLACE.

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

\$115,866.66 - \$144,833.78/annual

Internal Job Code

16009