

## CITY OF HAMILTON

**CORPORATE SERVICES DEPARTMENT**  
**(INFORMATION TECHNOLOGY DIVISION – INFORMATION TECHNOLOGY SECURITY - LOCATION - 55 YORK**  
**BLVD., 6<sup>th</sup> FLOOR)**

**INFORMATION SECURITY SPECIALIST**

**SUMMARY OF DUTIES**

Reporting to the Manager, IT Security, the Information Security Specialist provides expertise and leadership in strategy, design, development, review and management of security for all data, information, network and infrastructure systems across the Information Technology landscape and directs the full life cycle of network and application security management. This role is responsible for providing technical guidance and expertise to a team with a focus on the development and implementation of security policies, procedures and measures that ensure secure and reliable information systems across the corporation that are in compliance with existing data/information privacy laws and regulations.

The Information Security Specialist is responsible to manage, prioritize and organize workflow by leading a team while providing guidance and mentorship on tasks and projects.

The Information Security Specialist participates in large, complex projects with business and technology teams to deliver solutions aligned to changing business needs and strategies while considering existing technologies, security trends and tools, security architectures and changes in the IT landscape in order to provide current, relevant advice and guidance to the IS and business divisions of the City.

**GENERAL DUTIES**

Provides planning, input, technical direction and consultation for development and implementation of security policies and procedures, including information security compliance with legislations and industry standards.

Acts as a technical lead to define and develop security risk analysis scenarios and response procedures in collaboration with Infrastructure and Operations staff and the Manager, IT Security.

Defines and implements processes and methods for auditing and addressing non-compliance to information and/or network security standards.

Responsible to enforce security policies and procedures by administering and monitoring security profiles, reviewing security violation reports and investigating possible security exceptions, updates, maintains and documents security controls.

Oversees the configuration and maintenance of anti-virus software, firewalls, intrusion detection systems and other network security measures in collaboration with Infrastructure and Operations staff.

Acts as lead to educate IT and the business on security policies and provides consultation / advice on security issues regarding custom developed and packaged/managed systems.

Responsible to develop documentation and provides on-the-job training and coaching to IT staff for security and technology topics.

Acts as a technical lead and assists in the development, configuration, installation and troubleshooting of network systems (including wireless) to ensure security standards are met. The converged voice and data network includes servers, switches, routers and other computing network devices.

Represents the security needs of the City and its partner organizations by providing expertise and assistance in all IT projects with regard to security issues. Reviews system designs and architecture for potential risk areas and non-compliance and recommends methods to address security gaps.

Continually researches and maintains a current knowledge on the trends in software viruses and other attack/malware. Prepare communications and instructions to the City's user community on new security and virus threats including procedures for handling if infected.

Maintains a current knowledge and awareness of data and information privacy laws and regulations; monitors the City's compliance and recommends corrective action for non-compliance in collaboration with the City's business divisions.

Coordinates and performs periodic security assessments on all systems and networks as well reviewing all networking initiatives for security compliance. Analyzes results and provides recommendations to correct.

Responsible to research and evaluate IT security products and/or procedures, identifies, recommends and leads the adoption of those that will enhance/improve productivity and effectiveness of the City's network, data and application security.

May be assigned to an initiative or project requiring the individual to take direction from other IT Unit Manager and/or Project Manager.

May be required to provide on call support to users.

May be required to work extended hours to complete system maintenance

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.

Performs other duties as assigned, which are directly related to the major responsibilities of the job.

## **QUALIFICATIONS**

1. University Degree or College Diploma in Computer Science, Information Systems, Computer Technology or related discipline.
2. Industry security certification. CISSP from the International Information Systems Security Certification Consortium.
3. Seven (7) to ten (10) years of combined IT infrastructure/network and security experience.
4. Demonstrated strong problem-solving and leadership skills. Ability to make sound and logical judgements.
5. Extensive knowledge of Microsoft Active Directory, Azure AD and Azure Cloud Administration.
6. Extensive technical knowledge of client/server, network topology and network/infrastructure security.
7. Extensive knowledge and experience developing and implementing information security processes.
8. Strong knowledge and experience in network traffic analysis.
9. Demonstrated ability in configuring and maintaining anti-virus software, firewalls and intrusion detection systems.

10. Knowledge of network and infrastructure security issues, techniques and implications across multiple computer platforms and environments.
11. Strong knowledge of legislative requirements for security and privacy.
12. Knowledge and understanding of project management principles.
13. Experience in client and web-based application development and user support environments, including experience working with client and web-based applications technology, preferably in a municipal environment.
14. Working knowledge of relational database management system software (ORACLE, SQL Server along with Microsoft Access) and SQL (Structured Query Language).
15. Understanding of one or more standard computer programming and scripting languages commonly used in system administration (e.g. PowerShell, Python)
16. Knowledge of ITIL standards.
17. Must be able to communicate effectively, both orally and in written form.
18. Demonstrated ability to work effectively independently and as part of a team.
19. Proven leadership, analytical and problem-solving abilities.
20. Ability to make sound and logical judgments.
21. Strong interpersonal, customer service skills, written, and oral communication skills
22. Must possess a Class G Drivers' Licence.

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

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

\*\*\*\*\*