

CITY OF HAMILTON

CITY MANAGERS OFFICE

(INFORMATION TECHNOLOGY DIVISION – LOCATION – 55 YORK BLVD, 6th FLOOR)

CHIEF INFORMATION SECURITY OFFICER

SUMMARY OF DUTIES

Reporting to the Chief Information Officer (CIO), the Chief Information Security Officer (CISO) will be responsible for implementing and running the enterprise cybersecurity and technology infrastructure program.

The Chief Information Security Officer (CISO) is responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure information assets, technologies, and infrastructure are adequately protected. This includes oversight of the City's data center, network infrastructure, and telephony and related infrastructure across approximately 180 sites.

The CISO will lead efforts to secure the organization's information and IT assets by developing and implementing strategies to mitigate risks, ensure operational stability, manage security incidents, and ensure compliance with relevant policies and regulations.

The CISO will ensure that the business complies with all relevant IT security regulations and standards when acquiring new technology. This involves understanding the legal and regulatory landscape, assessing the technology's security features, and ensuring it meets the required compliance criteria.

The CISO will lead the IT Security and Data Operations Teams consisting of approximately 25 staff members.

GENERAL DUTIES

STRATEGY & PLANNING

Lead and provide strategic direction to achieve business goals by articulating standards, prioritizing technology initiatives and coordinating the evaluation, deployment, and management of current and future security and infrastructure technologies.

Participate in the development and implementation of IT strategies in collaboration with the IT Management team. Provide advice and recommendations to the Senior Management team on strategic infrastructure and security architectures and best practices to ensure the integrity of the City environment.

Develop and communicate security and technology plans and directions to senior management team, staff, partners, customers and stakeholders. Collaborate with the appropriate departments to develop and maintain a security technology plan that support organization risk assessment needs.

Direct development, execution and updating of cyber incident response and assist with technology business continuity planning and execution.

Design and develop enterprise security standards, architecture, security technology evaluation and implementation.

Review proposed infrastructure and application projects and solutions for compliance to defined City security and technology policies, procedures and standards.

Perform corporate cultural analysis and develop change strategies that are flexible and adaptive in collaboration with the IT Management Team to support effective adoption of new applications, technologies and related processes.

Conduct research and provide recommendations on security products, services, protocols, and standards in support of all infrastructure procurement and development efforts. Provide insight on emerging security technologies, trends and changes in the IT landscape. Identify and validate those security technologies that are right for the City and develop the best strategy for adoption and implementation. Maintain current knowledge of security industry trends and emerging technologies in anticipation of new business processes and system alterations.

Establish and manage delivery of quality service through the establishment and monitoring of Key Performance Indicators (KPI).

Devise strategies and make recommendations for enterprise information/data and solution architectures that meet the City's security objectives and goals, working in collaboration with City senior management team.

Coordinate with the IT Management Team to effectively and efficiently utilize IT resources – including personnel and equipment – across the IT organization.

Manage and maintain strategic relationships with the corporate departmental leadership - across the City with a view to sustained insight on City business strategies and directions and the provision of advice and guidance on opportunities for managing risk by complying with the City's security and infrastructure policies and procedures.

Oversee the support, management and administration of contracts for spending on services and products related to managed security hardware and applications. This includes overseeing the preparation and execution of requests for proposals (RFPs), bid proposals, contracts, and other documentation for security applications and hardware. Negotiates enterprise wide contracts with software and service providers as required and liaise with City vendors for prompt rectification of any security problems or emergencies. This will require the definition and facilitation of communication between the City and its providers in order to deliver products and services according to plan and within budget.

Participate in the evaluation, installation, configuration and deployment of new applications, systems software, products, and/or enhancements to existing applications to ensure compliance with the City's security policies.

Oversee the delivery of IT cyber and infrastructure related projects using standard project management practices and methods.

Validate the compliance of proposed new software against the City's security and infrastructure architecture and policies.

Plan, organize, and manage staff and overall section operations to ensure the stable operation of the City's IT security applications and software. This includes developing, maintain, supporting and optimizing key enterprise security hardware applications such as Antivirus, firewalls, etc.

Ensure 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.

Develop and manage operational and capital budgets to support strategic and operational requirements; conduct near and long-term financial forecasts for expanding functionality/user base.

Manage and maintain an inventory of company security application software and systems assets and their corresponding contracts/agreements.

Establish and maintain regular written and in-person communications with the organization's executives, department heads and end users regarding pertinent Security and IT activities.

Ensure effective management and communication of Security training and documentation for end users, hold clinics as necessary, and other user-related activities.

ACQUISITION & DEPLOYMENT

Assess and communicate risks associated with technology-related investments and purchases. Provide recommendations to mitigate the risks including identification of alternative solutions.

Develop business case justifications and cost/benefit analyses for technology spending and initiatives.

Define requirements for new technology implementations and communicate them to key business stakeholders.

Review hardware and software acquisition and maintenance contracts and pursue master agreements to capitalize on economies of scale.

Define and communicate corporate procedures, policies, and standards for the organization for acquiring, implementing, and operating new network systems, equipment, software, and other technologies.

Approve and prioritize projects and the project portfolio as they relate to the selection, acquisition, development, and installation of major information systems in collaboration with the IT Management Team.

Collaborate on the preparation of RFPs, bid proposals, contracts, scope of work reports, and other documentation for infrastructure projects and associated efforts with the Manager, Infrastructure & Operations.

Review the planned purchase of technology equipment and supplies for architecture compliance and that they meet operational requirements of the business.

Validate that the security, deployment, monitoring, maintenance, development, upgrade, and support of IT infrastructure systems, including networks, data centers, servers, PCs, operating systems, and associated hardware comply with documented standards.

Analyze existing operations and make recommendations for the improvement and growth of the IT infrastructure and IT systems.

OPERATIONAL MANAGEMENT

Design and direct the governance activities associated with ensuring compliance with the enterprise architecture.

Plan, develop and deploy security measures in collaboration with infrastructure, application and security resources.

Identify and research security technologies that are right for the City of Hamilton and develop/refine adoption strategies. Maintain current knowledge of industry trends and emerging technologies in anticipation of new business processes and system alterations.

Continually analyze/review and improve upon security technology standards across the organization to maintain a technological and competitive edge within the market and ensure compliance with the City security policies and procedures.

Direct the design and execution of vulnerability assessments, penetration tests, security audits, ensuring legislative compliance e.g. PCI compliance.

Provide continuous delivery of technical services through management of service level agreements with end users and monitoring of systems, programs, and equipment performance.

Ensure equipment and software operation adheres to applicable laws and regulations.

Convey the technology vision through the establishment and maintenance of regular written and in-person communications with the organization's executives, decision-makers, stakeholders, department heads, and end users regarding pertinent IT activities.

Coordinate with the IT Management Team to effectively and efficiently utilize IT resources – including personnel and equipment – across the IT organization.

Manage and develop operational and capital budgets and forecasts to support strategic and operational requirements in collaboration with IT Management.

Ensure that employees are provided with and use the appropriate equipment, material and/or procedures required to perform the assigned duties. Ensure that all employees perform work in accordance with applicable Health and Safety legislation and all City of Hamilton corporate and departmental policies and procedures. Ensure that appropriate action is recommended for those employees who do not work in compliance with legislation, policies and procedures.

Work 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.

Perform such other duties from time to time, as may be assigned by the IT Director, which are directly related to the normal job function.

QUALIFICATIONS

1. University Degree in field of Computer Science, Information Systems, or equivalent. Master's or PhD. degree in one these fields preferred.
2. Fifteen (15) years of relevant experience in the field with demonstrated leadership capability including 10 years direct experience managing and/or directing the direction, development and implementation of Cyber Security programs, security hardware, data centre and network operations.
3. Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Certified Information Systems Auditor (CISA), Certified in Risk and Information Systems Control (CRISC) or other similar credentials.
4. Familiarity with NIST or similar related Cybersecurity frameworks
5. Knowledge of network security practices and experience in interpreting the applicability of local and federal laws/regulations to City operations.
6. Strong knowledge of change management practices, business process flow analysis and re-engineering and methodology development.
7. Experience overseeing the design, development and implementation of change management facilitation programs and process review.
8. Experience with multi-platform environments, infrastructure and security architectures. Demonstrated experience in strategic security technology and network infrastructure planning, execution and policy development.
9. Experience in strategic technology planning, execution and policy development.
10. Knowledge across multiple technical areas and business segments relevant to the City's network and infrastructure architecture.
11. Knowledge of network and data security practices and experience in interpreting the applicability of local and federal laws/regulations to City operations.
12. Ability to prioritize and execute tasks in a high-pressure environment and make sound decisions in emergency situations.

13. Good Knowledge of the ITIL standard.
14. Strong technical knowledge of network and PC operating systems.
15. Strong technical knowledge of current network hardware, protocols, and standards including voice communications.
16. Knowledge of and experience in utilization of project management principles.
17. Knowledge of HR practices and policies relating to the hiring, retention and performance management of direct reports.
18. Exposure to business theory, business processes, management, budgeting, and business office operations.
19. Proven and problem-solving abilities.
20. Demonstrated strong leadership and personnel/project management skills.
21. Strong interpersonal, written, and oral communication skills.