JD ID A13516

CITY OF HAMILTON

CORPORATE SERVICES DEPARTMENT
(INFORMATION TECHNOLOGY DIVISION – INFRASTRUCTURE & SECURITY - LOCATION – 55 YORK BLVD., 6th FLOOR)

SUPERVISOR, NETWORK & SECURITY

SUMMARY OF DUTIES

Reporting to the Manager, Infrastructure & Security , the Supervisor, Network & Security is responsible for overseeing the enterprise security and network solutions, for voice, data, telephony and cloud. Provides direction and advice for appropriate security and connectivity services to connect systems while focusing on the design and development of network and security solutions, network integration, voice and data . Provides network and security management services to manage the networks for optimal security, performance and capacity, system tuning, development and implementation of solutions, performance analysis in support of networks, availability management, asset management and security management.

The Supervisor will provide leadership, guidance, and day to day management of the work and performance of a combined team of analysts supporting Security and Network, services including Corporate Trunked Radio network and devices.

The Supervisor leads security and network analysis and contributes to the design on medium to large, complex projects that span or impact multiple technical environments and require knowledge or insight on multiple security and technology areas and communication protocols. The Supervisor, Network & Security may be assigned on one or more projects as a project team member and/or a project lead that require knowledge or insight on multiple business and/or technology areas.

GENERAL DUTIES

Manages and leads the development, configuration, installation, maintenance and troubleshooting of security and network systems, wireless solutions, and telecommunications to meet the functional objectives of the business. Utilizes remote monitoring tools to provide stable, dependable and secure network services across multiple platforms. Includes monitoring of multiples networked sites/locations where networks are deployed.

Provides direction, leadership and day to day management to a contingent of staff including daily supervision, scheduling, skills development and disciplinary actions including extended after-hours support.

Responsible for establishing an enterprise security policies and process, architecture and training.

Responsible for selecting the appropriate security solutions, and oversight of any vulnerability audits and assessments.

Responsible for development and communication of a corporate security vision that will result in achieving higher levels of enterprise security.

Accountable for creating and maintaining enterprise’s security and network architecture design, enterprise’s security awareness training program.

Accountable developing and maintaining the enterprise’s security and network policies, standards, baselines, guidelines and procedures.

Accountable to develop and maintain the enterprise’s Business Continuity Plan and Disaster Recovery Plan, where appropriate.

Maintains up-to-date knowledge of the IT security industry including awareness of new or revised security solutions, improved security processes and the development of new attacks and threat vectors.

Selects and acquires additional security solutions or enhancements to existing security solutions to improve overall enterprise security as per the enterprise's existing procurement processes.

Oversees the deployment, integration and initial configuration of all new security solutions and of any enhancements to existing security solutions in accordance with standard best operating procedures generically and the enterprise's security documents specifically.

Ensures the confidentiality, integrity and availability of the data residing on or transmitted to/from/through enterprise workstations, servers and other systems and in databases and other data repositories.

Supervises all investigations into problematic activity and provides on-going communication with senior management.

Supervises the design and execution of vulnerability assessments, penetration tests and security audits.

Performs regular security awareness training for all employees to ensure consistently high levels of compliance with enterprise security documents.

Conducts staff performance reviews, regular coaching, mentoring and counselling (including extended after-hours support) skills development and management of overall performance.

Leads the hiring process and conducts interviews, prepares candidate exams and actively participates in selection process.

Manages and maintains technologies, LAN/WAN/wireless/voice operations, and telephony application environments working collaboratively with network, facility and hardware/software vendors to ensure timely problem resolution. Maintains and utilizes platforms, server and network management applications to identify network faults, to ensure the provision of data or other telecommunications access to customers, and the movement of information from one location to the other.

Manages and reviews issues and problem logs relating to infrastructure and network operations, groups and prioritizes outstanding issues and develops resolution plan. Maintains strong communications with IS and business leaders on network availability and planned shutdowns.

Executes the role of Customer Relationship Manager and IT liaison as required.

Collaborates on the designs of the security and network architecture, design of security and network infrastructure, and plans and designs LAN/WAN/wireless and voice solutions.

Responsible for collaborating with Security Specialist and technical architect on the development and implementation of security policies and procedures (e.g., user log-on and authentication rules, security breach escalation procedures, security auditing procedures and use of firewalls and encryption routines).

Develops and manages capacity and resource plans, assessing network risks and developing risk management strategy and contingency plans.

Monitors budgetary accounts in accordance with established corporate policies and procedures. The Supervisor also manages day to day financial expenditures.

Collaboratively develops section goals, work plans and objectives by participating in strategic planning sessions.

Acts on behalf of Manager in his/her absence as required.

Researches industry standard best practices for Security and Network Infrastructures; manages the implementation of

appropriate security patches and upgrade to Network technologies in collaboration with the Security Specialist.

Performs industry analysis necessary to determine best practices and define/select processes and tools.

Analyses and tests network performance and provides network performance statistics and reports; develops strategies for managing and maintaining network infrastructure.

Maintains and analyzes an inventory of assets; identifies opportunities for corporate and department efficiencies and improvements and makes recommendations for optimization of asset use to IS Management Team.

Provides project and/or workstream duration and effort estimates for infrastructure/network component design, installation and operation activities to the Project Managers and business owners for current and capital projects of medium complexity.

Conducts research and provides recommendations to management on products, services, protocols, and standards in support of all infrastructure procurement and development efforts.

Provides insight and direction on emerging technologies, trends and changes in the IT Security landscape. Identifies and validates those technologies that are right for the City and develops the best strategy for adoption and implementation.

Collaborates with database and systems analysts to develop, implement and maintain a thorough Disaster Recovery Plan and back-up strategy for all corporate data.

Oversees and coordinates activities relating to researching, analysing and implementing software patches and/or hardware changes to fix identified network deficiencies.

Defines and develops and implements operational processes in collaboration with IS Management.

Manages and maintains vendor service level agreements for security, hardware, software and connectivity in accordance with the City's procurement policies and monitor compliance.

Reviews and approves expenditures to network and security hardware, software, licenses and supplies to meet operational requirements.

Contributes to the development of the annual work plans ensuring consistency with divisional and corporate strategic plans as requested by the Manager.

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

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.

Performs other duties as assigned which are directly related to the responsibilities of the position.

QUALIFICATIONS

1. University Degree or College Diploma in Computer Science, Information Systems, Computer Technology or related discipline or an equivalent combination of education and relevant business experience.

2. One or more of the following certifications:
    a. GIAC Security Essentials Certification
    b. GIAC Security Leadership Certification
    c. ISACA Certified Information Security Manager
    d. Microsoft Certified Systems Engineer: Security
    e. $(ISC)^2$ SCCP
    f. $(ISC)^2$ CISSP
    g. $(ISC)^2$ ISSAP

3. Five to seven years experience in security and infrastructure/network environments in security and network design, implementation, administration and support. Demonstrated previous experience in a supervisory or lead capacity.

4. Extensive experience in network and security technologies, installing, configuring, maintaining and supporting networking components including switches and routers.

5. Demonstrated understanding and experience working with network hardware equipment configuration, set-up and familiarity with test equipment.

6. Extensive experience in client/server and operating systems, including Windows Operating System (Windows 10, Server 2012/2016), and working knowledge of Linux.

7. Extensive experience installing, configuring, maintaining and supporting datacentre hardware (servers, blades, tape and virtual libraries, UPS and mobile, wireless technologies and architectures.

8. Extensive experience with VoIP and working knowledge of other telecommunication network systems.

9. Demonstrated ability to lead small teams to deliver to project schedule on time and with quality.

10. Demonstrated skills in analysis, planning and logical troubleshooting.

11. Demonstrated skills in application and hardware virtualization and mobile, wireless technologies and architectures.

12. Good Knowledge of the ITIL standard.

13. Knowledge and understanding of project management principles.

14. Strong working knowledge of network protocols, and standards such as Ethernet, LAN, WAN, VoIP, DSL, TCP/IP, T1, 802.11x, and Fibre Optics.

15. Strong working knowledge of networking systems (DNS, WINS, Active Directory), protocols, and standards such as Ethernet, LAN, WAN, VoIP, DSL, TCP/IP, T1, 802.11x and Fibre Optics.

16. Experience in client/server and operating systems, including Windows Operating System working knowledge of Linux and DNS, WINS, Active Directory (LDAP). Windows 10, Server 2012/2016).

17. Knowledge of the configuration, installation, maintenance and troubleshooting of servers, including routers and switches, e-mail, print and backup servers and their associated operating systems and software.

18. Experience configuring and maintaining anti-virus software, firewalls, intrusion detection systems and other network security measures.

19. Experience with installing, configuring, maintaining and supporting email technologies and protocols, including Exchange Server, Mobile Device Management, Office 365 (hybrid Cloud environments).

20. Strong leadership skills.
21. Ability to make sound and logical judgments.
22. Strong interpersonal, written and oral communication skills.
23. Class G Drivers' License required.

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.

* * * * * * * * * * * * * *