Technical Services and Security Coordinator

Full Time – Non Union

<div align="right">

2022-NON-GG-327
</div>

The County of Hastings is currently accepting applications for a **Full-Time Non-Union TECHNICAL SERVICES AND SECURITY COORDINATOR** for the Information Technology Department at the County Administration Building in Belleville, Ontario.

The role of the Technical Services and Security Coordinator is to ensure the secure operation of the in-house computer systems, servers, and network connections.

RESPONSIBILITIES:

1. Deploy, manage and maintain all network security systems and their corresponding or associated software, including firewalls, intrusion detection systems, and anti-virus software to mitigate any risks associated with security breaches.
2. Administer and maintain end user accounts, permissions, access rights including all aspects of enterprise directory services and supporting server infrastructure.
3. Ensure security and confidentiality by maintaining servers, including e-mail, print, MDM, and backup servers and their associated operating systems and software.
4. Maintain all network hardware and equipment, including routers, firewalls, switches and UPSs.
5. Manage and maintain connection security for local area networks, the company Web site, the company intranet, and Microsoft 365 environments.
6. Ensuring integrity and confidentiality of sensitive data across the organization including but not limited to Payroll, Human Resources and Administration.
7. Maintain and ensure the security and confidentiality of databases and data transferred both internally and externally.
8. Participate in the creation of enterprise security documents (policies, standards, baselines, guidelines and procedures) under the direction of the Technical Services and Security Supervisor, where appropriate.
9. Draft, implement and maintain policies, procedures and associated training plans for network resource administration, appropriate use, and disaster recovery.
10. Perform 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.
11. Maintain up-to-date baselines for the secure configuration and operations of all in-place devices, whether they be under direct control (i.e., security tools) or not (i.e., workstations, servers, network devices, etc.).
12. Monitor and test network performance and provide network performance statistics and reports.
13. Participate in the design and execution of vulnerability assessments, penetration testing, as well as server and security audits.
14. Conduct research on network products, services, protocols, and standards in support of network procurement and development efforts.
15. Ensure network and IP connectivity of all workstations, servers, and back-end office infrastructure.
16. Practice network asset management, including maintenance of network component inventory and related documentation and technical specifications information.
17. Audit and monitor server logs, firewall logs, intrusion detection logs, and network traffic for unusual or suspicious activity. Interpret activity and make timely recommendations for resolution.
18. Recommend, schedule, and perform network improvements, process improvements, upgrades, and repairs.
19. Identify risks, recommend, schedule (where appropriate), and apply fixes, security patches, disaster recovery procedures, and any other measures required in the event of a security breach.
20. Perform file system configuration and management; define and perform server backups and recovery procedures.
21. Plan and implement server upgrades, maintenance fixes, and vendor-supplied patches.
22. Plan, design and upgrade network installation projects
23. Serve as technical lead in network problems and emergencies. Troubleshoot and resolve network problems.
24. Monitor and maintain current virtual server and virtual desktop environment. Deploy patches upgrades and fixes as required.
25. Work with third party vendors for maintenance/upgrades of existing systems where required.
26. Provide on-call support for end users for all in-place security solutions.
27. May be required to work after normal hours to perform certain tasks.

28. Other duties as may be required from time to time.

QUALIFICATIONS:

1. Minimum 3 year College diploma or university degree in the field of computer science and/or a minimum of 7 years equivalent work experience.
2. Security system and network maintenance experience preferred.
3. Strong understanding of IP, TCP/IP, and other network administration protocols.
4. Understanding of various network topologies including VLANS and VOIP.
5. Working technical knowledge of network and PC operating systems, including:
   - Protocols and standards such as Ethernet, LAN, WAN, ARP, TCP/IP, DNS, SIP, etc.
6. Skilled at installing/configuring L2/L3 switches, routers, firewalls, etc.
7. Extensive knowledge of anti-virus/anti-malware detection systems, FortiGate firewalls, intrusion detection systems, and other network security measures.
8. High level of analytical and problem-solving abilities and the associated ability to forecast or predict network security concerns.
9. Significant ability to maintain confidentiality.
10. Ability to work in high-pressure, time sensitive situations where server/network connectivity downtime must be kept to a minimum.
11. Ability to conduct research into security issues and products as required.
12. Knowledge and experience working with VPN connections across multiple locations.
13. Knowledge and experience with storage technologies such as SAN or NAS.
14. Thorough knowledge of Microsoft domains, Microsoft Active Directory, Microsoft Azure and Microsoft Servers, in both physical and virtual server environments.
15. Experience with Microsoft 365 and Microsoft SQL Databases is required.
16. Knowledge and working experience with the following Operating systems; Windows 7,10, Windows Server 2012, 2016, and 2019.
17. Knowledge and experience working in a Virtual environment using vSphere and VMware (server and desktop).
18. Must have a valid driver's license and reliable transportation for travel to remote sites.

WAGE RANGE: $62,464 - $73,056 per annum, with excellent fringe benefits

HOURS OF WORK: Monday – Friday, 8:30-4:30, 35 hours per week

Please forward applications to: Colleen Dunham
A/Human Resources Advisor
Talent Management & Acquisition
careers@hastingscounty.com

Please quote "**2022-NON-GG-327 – "your name**" in the subject line