Hamilton Public Library

Freedom to Belong and Discover

Please send application to recruit@hpl.ca no later than 11:59pm on Thursday, September 25, 2025. Please quote job title, department or location, and position number.

JOB TITLE:	**IT Infrastructure Specialist – Permanent Full Time – 2 Positions**
PAY BAND:	Grade 5 (Professional Exempt) $51.082 to $63.854 hourly
LOCATION:	Digital Technology, Central Library Travel to conduct library business will be required
SCHEDULE:	35 hours per week; May include evenings and weekends as operationally required.
START DATE:	As soon as possible

JOB SUMMARY:

Reports to the Manager, Digital Technology Infrastructure; Responsible for the development, administration, and support of services within the following portfolios: Systems Administration, network and domain administration, client computer configuration, Wireless infrastructure administration, application configuration and implementation, back-up, and disaster recovery; Participates in general departmental activities including IT service desk support.

JOB DUTIES:

- Manage, maintain, and upgrade servers, networks, domains, and databases to ensure optimal performance and security.

- Serves as lead for assigned applications, projects and technologies; acts as the primary resource person for DT infrastructure team

- Reviews services and operations for relevance and responsiveness; presents recommended changes; plans and schedules service expansions and enhancements; recommends objectives and outcomes; participates in strategic planning and library projects;

- Administer and optimize SaaS firewalls and network services to ensure secure and efficient operations.

- Enhance the organization’s cybersecurity posture by implementing and enforcing security policies, conducting regular audits, and responding to threats.

- Manage HPL’s Microsoft 365 environment, user account and license management, configuring and troubleshooting Microsoft 365 services, implementing and enforcing security and compliance policies, and collaborating with teams on projects and strategy.

- Responsible for managing user access and authentication, enforcing strong password policies, monitoring for suspicious activity, and implementing identity management solutions to protect sensitive data and prevent unauthorized access.

- Manage organization wide anti-virus systems and disaster recovery processes.

- Responsible for running backup and restore operations: managing backup software and hardware, troubleshooting issues, conducting regular audits and tests, coordinating with other DT teams, and documenting procedures to meet compliance and business continuity goals.

- Liaise with vendors for repairs, updates, and support.

- Evaluate and recommend new technologies, equipment, and processes to meet business needs.

- Collaborates on the planning, scheduling and purchasing of applications and technology.

- Analyzes service incidents and problems, identifies risks, provides recommendations, and implements solutions in relation to assessed business needs.

- Provide technical support, training, and documentation for staff and the public.

- Plans, organizes, schedules and coordinates teamwork.

- Performs other duties as assigned as related to the major responsibilities of the job.

MINIMUM QUALIFICATIONS:

Educational Requirements:

- A Bachelor’s Degree in Computer Science or Information Technology, normally obtained through a three (3) year University degree or equivalent combination of education and experience.

- Preferred certifications: ITIL, Microsoft Azure, VMware, Citrix, or other networking certifications.

Experience:

- Configure and manage IT infrastructure, including physical servers, virtual machines, storage systems (SAN), operating systems, backups, and security tools.

- Minimum of three (3) years hands-on experience with:
  - Citrix Virtual Desktops (VDIs) and virtualized applications.
  - WLAN controllers and wireless access points.
  - Windows Server, VMware ESXi, VMware vCenter.
  - Microsoft 365 (implementation, management, and troubleshooting for Entra ID, Teams, Outlook, OneDrive, etc.).
  - Administration of Microsoft 365 environment including security policies
  - Firewall configuration, management, and monitoring.
  - SAN firmware upgrades, storage management, and maintenance.
  - Software deployment and inventory management using SCCM.
  - Veeam backup software and daily backup management.
  - Networking equipment like firewalls, routers, and switches.

- Experience with application administration and support (preferably in a library environment).

- Strong understanding of ITIL practices.

- Valid Ontario driver’s license with a driver’s abstract satisfactory to the Employer.

Skills and Competencies:

- **Communication:** Strong written, verbal, and listening skills.
- **Customer Service:** Commitment to excellent service and understanding diverse needs.
- **Judgment:** Problem-solving, anticipating consequences, and proposing solutions.
- **Continuous Learning:** Staying updated with policies, technologies, and best practices.
- **Technical Knowledge:** Proficiency in:
  - Windows Server, Active Directory, and DNS.
  - Networking protocols (Ethernet, LAN, WAN, VoIP, TCP/IP, etc.).
  - VMware, Citrix, and server virtualization.
- **Leadership:** Team leadership, adaptability, and a positive attitude in a changing environment.
- **Project Management:** Effective resource management and project implementation.
- **Results Orientation:** Strong prioritization, goal-setting, and teamwork skills.

Physical Requirements:

Physical ability and stamina to operate relevant equipment, to retrieve materials and to perform tasks involving the lifting and movement of library materials and equipment

Legislative Requirements:

Works in accordance with all applicable Occupational Health and Safety, Employment Standards, Human Rights, Labour Relations and Pay Equity legislation and all other relevant legislation

Organizational Requirements:

Adheres to policy and legislation identified in the Hamilton Public Library Policy and Procedures Manuals

HPL employees and users of HPL cloud-based applications are required to use Multi-Factor Authentication (MFA) as an essential measure to enhance the protection of HPL's technology assets. MFA augments technological security by requiring two steps for full authentication. Employees who do not have a Library-provided cellphone are expected to use their personal cellphone or internet connected device to satisfy the MFA requirement consistent with HPL policies and procedures.

Please be aware the selection process may involve any of interviews, test, and presentations or any combination thereof.

The Hamilton Public Library is an equal opportunity employer that is committed to inclusive, barrier-free recruitment and selection processes. If contacted for an employment opportunity, please advise Human Resources if you require accommodation.