Legislative Assembly Service

SASKATCHEWAN

If you are interested in this opportunity, please submit a cover letter and resume by 5:00 p.m. (CST) **August 26, 2025** to:

Manager, IT Services
Attention: Holly Schafer
Room #33 - 2405
Legislative Drive Regina,
SKS4S 0B3
Tel: (306) 787-8883
E-mail: careers@legassembly.sk.ca

Please quote competition 1050417 in the subject of your email.

Clearly indicate in your resumé or cover letter where and how you have gained the required knowledge and qualifications. Selections for interviews will be based on this information.

Thank you for your expression of interest. Only candidates selected for interview will be contacted.

To learn more about the LAS, our Vision, Mission and Values, and to find further information about the position, salary and benefits, please visit https://www.legassembly.sk.ca/las/employment/

Security Analyst (Permanent, Full-time, on site) **anticipatory*

Imagine working at the heart of Saskatchewan's democratic process, where your IT skills don't just serve an organization—they sustain a parliamentary institution. Based in the historic Legislative Building in beautiful Wascana Park, this role offers the chance to grow, evolve, and contribute to something bigger. The Legislative Assembly Service (LAS) is dedicated to enhancing parliamentary democracy by providing impartial, non-partisan support to the Legislative Assembly. Our mission is to foster a transparent, participatory democracy, with a team committed to supporting the institution of Parliament for the people of Saskatchewan.

**The Legislative Assembly Service is evolving its IT structure to support long-term organizational needs. We are hiring one position — either a Security Analyst or an IT/Server Analyst — based on the strengths of the candidate pool. This role is essential to ensuring a secure, high-performing IT environment that supports the work of Members and the Assembly.*

Reporting to the Manager of Information Technology Services, the Security Analyst is responsible for monitoring, analyzing and responding to security threats and vulnerabilities to mitigate security risks and protect enterprise IT systems and data.

What You'll Do:

- Monitor networks, systems, and applications for suspicious activity, security breaches, potential vulnerabilities and collaborate with security service providers to respond to threats in real time.
- Implement and maintain security controls (e.g. firewalls, IDS/IPS, endpoint protection, and automated detection systems).
- Conduct risk assessments and vulnerability scans, prioritizing risks, and recommending appropriate safeguards.
- Lead or support incident response and disaster recovery efforts with ITS and external partners.
- Develop and enforce security policies, procedures, and user awareness training.
- Support technical teams with implementing security safeguards, such as patching, anti-malware, secure configuration, and access controls.
- Administer and monitor security tools, ensuring systems are current and threat aligned.
- Ensure secure design, deployment, and operation of applications and infrastructure.
- Perform audits, compliance reviews, analyze anomalies and develop corrective actions.
- Develop scripts, tools, and procedures to automate monitoring, scanning, and reporting.
- Stay current on cybersecurity threats and advise ITS leadership on risks and strategy.

What You Bring:

- Bachelor's degree in Cybersecurity, Information Security, or a related field, combined with three or more years' experience in cybersecurity roles—preferably in a public sector or enterprise-level IT environment.
- In In-depth knowledge of Security principles and technologies (IAM, IDS/IPS), Risk assessment methodologies, Security information and event management (SIEM) systems, malware detection and remediation tools.
- Working knowledge of IT network infrastructure components, secure coding practices and basic scripting, change management processes and IT service management tools.

This role demands strong analytical thinking, discretion, and sound judgment in protecting sensitive systems and data. Certifications such as Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), or Certified Ethical Hacker (CEH) are preferred.

All employees of the Legislative Assembly Service are required to provide non-partisan, confidential service to all Members of the Legislative Assembly and the successful candidate will need to provide a satisfactory criminal record check.