SGEU Up-in-Range

The following posting is in accordance with the clauses dealing with "In-Hiring Rate of Pay".

Permanent Full-time
INF004989 - Senior Cyber Security Analyst
Ministry: Non-Executive Government>537 Saskatchewan Public Safety Agency
Grade and Job: SGEU.11., SSE - SGEU
Salary Range: $44.534 - $53.882
Rate Approved: $51.00 per hour

Key Responsibilities of position:

As a Senior Cyber Security Analyst, you will be responsible for:

- Provide subject knowledge and expertise in the design, delivery and documentation of Cybersecurity solutions.
- Assist with the development and implementation of Business Continuity and Disaster recovery plans and processes for systems and services critical to the delivery of services provided by the SPSA.
- Lead and coordinate security aspects of Business Continuity and Disaster Recovery processes. Develop and coordinate table-top exercises that practice Business Continuity and Disaster recovery processes and conditions.
- Respond to escalated potential incidents from multiple sources which includes SPSA internal users, PECC staff and users, external security services providers and other agencies covered under the SPSA service delivery programs and service.
- Support infrastructure teams by ensuring designs follow set security policies and ensuring technical designs comply with cybersecurity principles.
- Actively participate in industry and vendor working groups and development sessions.
- Work with a diverse set of cloud and on-premise security tools, providing recommendations on configuration and upgrade options when necessary. Lead threat hunting activities in our cloud and on-prem environments to detect and isolate potential threats and provide mitigation recommendations.
- Maintain an awareness of existing and proposed security-standard-setting groups, federal, provincial and international legislation and regulations pertaining to information security.
- Coordinate with relevant operational groups and service providers to set up, implement, and maintain identity and access management measures to prevent or detect security incidents or breaches.
- Execute Security Threat and Risks Assessments including High Level Security Assessment (HLSA) on vendors, Statement of Sensitivity (SoS), Overseeing regular Vulnerability and Penetration Testing and Reporting of SPSA Infrastructure.
- Provide specialized technical knowledge during RFP processes. Participates in the development of complex RFP’s for the procurement of products and services. Creates and updates the

technical RFP requirements. Participate as a member of the decision-making team in the evaluation of RFP responses and recommendations.

- Provide support in the development of options papers, business cases and supporting documentation towards project development and strategic planning activities involving infrastructure and enterprise system deployments.
- Maintain knowledge of emerging technological trends and utilizes this knowledge to educate both IT and the business on opportunities to build better IT solutions that support and drive business decisions.
- Participate in the definition of the architecture and technology needs of the organization based on new and emerging technologies.

The successful candidate will have a Degree or diploma in Computer Science or related field from a recognized institute and at least 5 years' experience in an information technology, infrastructure support and enterprise system management capacity with a focus on IT Security and Cybersecurity.

You will have knowledge of:

- Acts/Regulations/ Legislation
- Organizational programs, standards, policies and expectations.
- Current IT Security and Cybersecurity fundamental standards and frameworks.
- Documentation strategies and models
- Business requirements analysis and gathering to optimize/and or to develop IT solutions.
- Requirements analysis and solution design techniques.
- IT Infrastructure Fundamentals
- Cybersecurity applications and systems
- Information analysis techniques.
- Enterprise systems
- Cybersecurity standards
- Business Continuity concepts and models

Qualifications of person Appointed:

- 15+ years' experience including a strong level of understanding and practical experience on the governance and compliance elements of Cyber Security. Excellent level of understanding and applied experience with a broad range of Cyber Security tools/software and vendors.
- Practical and working knowledge on business continuity and disaster recovery from both a planning perspective and exercises.
- Bachelor in Computer Science / ISC2 Cybersecurity Accreditation / ITIL Certified / ISO ISMS Foundation
- Certified Ethical Hacker / Certified Security Analyst / Business Continuity Professional designation

Submit challenges to staffing@gov.sk.ca

Closing Date: December 5, 2025