

IDENTIFICATION

Department	Position Title	
Workers' Safety and Compensation Commission	Senior Security Systems Specialist	
Position Number	Community	Division/Region
97-9991	Yellowknife	Performance and Corporate Services

PURPOSE OF THE POSITION

The Senior Security Systems Specialist is responsible for the analysis, planning, development, maintenance, and improvement of the procedures, policies governance, support of Workers' Safety and Compensation Commission Security Architecture.

SCOPE

The Workers' Safety and Compensation Commission (WSCC) is a Crown Corporation of the Governments of the Northwest Territories and Nunavut that is directed by a Governance Council through the President & CEO. WSCC operations are located in Yellowknife and Iqaluit.

The WSCC promotes safe workplaces through education and prevention, and cares for injured workers through a system of no-fault compensation. The system is funded through the collection of assessments from employers and is governed by the *Workers' Compensation Acts* of the Northwest Territories and Nunavut.

The WSCC is committed to an environment free of racism and discrimination, where people feel safe when receiving services. This can be achieved by respectful engagement that acknowledges the importance of cultural differences and values Cultural Safety.

The WSCC Information Technology Infrastructure, critical for operations, spans multiple offices and territories, handling diverse data requirements. With an annual budget exceeding \$5M, it emphasizes the need for continual high performance and reliability, reflecting the network's complexity across various territories.

Located in Yellowknife the Senior Security Systems Specialist (Specialist) report to the Manager Information Technology and Business Intelligence and provides specialized services to active WSCC employees in Yellowknife and Iqaluit.

The Specialist provides comprehensive analysis, planning, development, maintenance, and enhancement of all governance and security processes, policies, and implementation of Security Infrastructure. The scope of duties includes assisting in the development of information security related policies, procedures, standards, and guidelines which govern information management (IM), information systems (IS) and information technology (IT). This involves establishing a baseline of WSCC information security, and consulting with divisions to understand their business functions and interpret their appetite and tolerance for risk and translate that into an actionable desired future state.

The Specialist will work directly hands on implementing security measures on the infrastructure or applications but will work closely with the divisional teams that have responsibility for maintaining these assets to ensure they understand the requirements which must be addressed, and to provide advice and guidance on implementation of best practices to ensure the most effective implementation of information security measures and practices. This position is responsible for leading the development of WSCC's Incident Response and Investigations framework, ensuring swift and effective security incident management. They will manage and conduct comprehensive security posture assessments, implement awareness training, and enforce standard compliance to fortify the organization's cybersecurity resilience.

As a member of the Information Services team the Senior Security Systems Specialist is required to interact professionally with clients in all situations. With expertise in security and systems administration, the Specialist provides input into the Information Services Strategic Plan and contributes to initiatives related to the Plan.

The incumbent is required to address service incidents that may heavily impact the operation of the WSCC, and therefore may require rapid response and resumption of service. These incidents may occur any time, 24 hours a day, 365 days a year. The incumbent may be required to be on-call for extended periods or on a rotational basis 24/7 to ensure the reliability of the network.

This position may require the incumbent to work flex time to support regions. Duty Travel to regional communities will be required from time to time.

- Supporting activities of the above responsibility.

RESPONSIBILITIES

1. Provides a high level of leadership in the security administration for all users within and outside the Workers' Safety and Compensation Commission (WSCC) network:

- Implement and uphold compliance with security administration procedures to secure WSCC server and storage systems for all users within and outside the WSCC network.
- Establish and enforce standards for server, storage and network security controls, maintenance, access, and security procedures.
- Design and implement controlled data access for external entities without compromising the integrity and security of WSCC data repositories.

- Manage security processes and protocols, ensuring secure application access to data systems, email, and remote applications.
- Stay abreast of technological advances in server and storage management, contributing to decisions enhancing security, performance, stability, and supportability.
- Provide leadership in maintaining the security systems.
- Investigate and lead the resolution of security breaches.
- Perform standard and non-standard security administration tasks, resolving security issues.
- Collaborate with the Manager, Information Technology, Senior Server and Network Specialist and WSCC colleagues, and contractors to implement and support network security procedures.

2. Leads and implements the Security Governance:

- Participate in the operation of information security technologies including, but not limited to, Network Intrusion Prevention and Detection Systems, Enterprise Anti- Virus Systems, Enterprise Host Intrusion Prevention Systems, Firewalls, Patch Management Systems, End Point Encryption, Point Protection and Security Incident Management systems.
- Lead in security incident response action(s): coordinating remediation and recovery actions, disseminating information to stakeholders, and working with incident response consultants.
- Work closely with the Senior Server and Network Analyst in the Information Technology team to ensure the security of WSCC technology infrastructure.
- Lead the creation and enforcement of policies, procedures, standards and guidelines and associated plans for information security and access controls based on industry best practice and managerial direction.
- Assist the Information Technology team in the creation and review of disaster recovery and business continuity plans dealing with loss of technology or departmental applications.
- Lead security reviews, vulnerability assessments, penetration tests and risk assessments of infrastructure or systems. This may be done in coordination with an external professional security services firm or consultant.
- Deliver, or work with the Manager of Information Technology and/or a consultant to deliver, information security training and awareness programs throughout the WSCC.

3. Provides expertise and support in configuration, implementation, and maintenance of complex networks.

- Evaluate, plan, and implement network infrastructure to guarantee seamless connectivity and optimal performance across WSCC departments and communities.
- Collaborate with stakeholders to define network requirements, offering informed recommendations.
- Troubleshoot and resolve complex network issues in coordination with relevant teams.
- Design and implement network security measures and protocols.
- Lead in developing and maintaining comprehensive network documentation.

- Stay informed on technological advancements in network infrastructure, contributing to strategic decisions for optimal network performance.
- Collaborate with the broader WSCC team and external partners to enhance network services.

4. Participates and leads in periodic formal audits and milestone reviews:

- Ensure that the overall integrity, security, and accessibility of data are maintained.
- Contribute to and maintain a consistently high standard of documentation.
- Assist in preparing reports, recommendations, or alternatives that address existing and potential trouble areas in operating systems.
- Create systems models, specifications, diagrams, and charts to provide direction to in-house and outsourced developers.
- Ensure service standards are met in business solutions.

WORKING CONDITIONS

Physical Demands

No unusual demands.

Environmental Conditions

No unusual conditions.

Sensory Demands

No unusual demands.

Mental Demands

No unusual demands.

KNOWLEDGE, SKILLS AND ABILITIES

- Knowledge of systems security administration, as well as information security practices and procedures.
- Knowledge of firewalls, intrusion prevention and detection systems, enterprise anti-virus software, and enterprise patch management systems.
- Knowledge of information security best practices as it relates to development of custom software applications.
- Knowledge of information security and privacy legislation in a Canadian context.
- Knowledge of common protocols such as TCP/IP, SNMP, HTTP, Radius and broad understanding of cryptography technologies/protocols including Kerberos, PKI, and AES/DES.
- Familiarity with systems development life cycles (SDLC) and the integration of information security best practices within a SDLC.
- Skills relating to Network Intrusion Prevention and Detection Systems, Enterprise Anti-Virus Systems, Enterprise Host Intrusion Prevention Systems, Firewalls, Patch Management

Systems, End Point Encryption, Point Protection and Security Incident Management systems.

- Skills and knowledge relating to Information Security Management Systems, control frameworks (COBIT, ISO 27001, NIST CSF) and related risk assessment methodologies (CIS, PCI, HIPPA, HIA etc.)
- Analytical skills and problem-solving abilities.
- Ability to conduct research into security issues and products, as required.
- Ability to evaluate, plan, and implement network infrastructure to guarantee seamless connectivity and optimal performance across WSCC departments and communities.
- Interpersonal, communication and organizational skills.
- Attention to detail and accuracy.
- Ability to negotiate, persuade and find compromise between stakeholders.
- Ability to develop oneself professionally to meet the security needs of the organization.
- Ability to remain calm and focused during difficult situations.
- Ability to commit to actively upholding and consistently practicing personal diversity, inclusion and cultural awareness, as well as safety and sensitivity approaches in the workplace.

Typically, the above qualifications would be attained by:

A degree in Engineering, Computer Science, Cyber Security, Information Technology, or Information Management program; and four (4) years of relevant experience including two (2) years within the field of Information or Network Security and Security Governance.

Equivalent combinations of education and experience will be considered.

ADDITIONAL REQUIREMENTS

Position Security

- No criminal records check required
- Position of Trust – criminal records check required
- Highly sensitive position – requires verification of identity and a criminal records check

French language (check one if applicable)

- French required (must identify required level below)
Level required for this Designated Position is:
ORAL EXPRESSION AND COMPREHENSION
Basic (B) Intermediate (I) Advanced (A)
READING COMPREHENSION:
Basic (B) Intermediate (I) Advanced (A)
WRITING SKILLS:
Basic (B) Intermediate (I) Advanced (A)
- French preferred

Indigenous language: To choose a language, click here.

- Required
- Preferred