Government of
Northwest Territories

IDENTIFICATION

Department	Position Title	
FINANCE	Senior Courts & Security Technology Specialist	
Position Number	**Community**	**Division/Region**
15-14718	Yellowknife	Application Services /HQ

PURPOSE OF THE POSITION

The Senior Courts and Security Technology Specialist provides the senior technical knowledge and expertise necessary to support the design, implementation, maintenance and operations of technology enabled facility security and courtroom operational services used by the Department of Justice and the Judiciary.

SCOPE

Located in Yellowknife, the Senior Courts and Security Technologyl Specialist reports to the Manager of Courts & Security Technical Services in the Application Services division of the Department of Finance.

The team is responsible for the technology-enabled systems used by facilities, such as the NWT Courthouse and NWT correctional facilities. These systems include:

- Courtroom technology systems including audio video and digital transcription services.
- Access and door control systems;
- Camera and surveillance systems;
- Automated evacuation route systems;
- Radio, Intercom and secure telephone systems;
- Inmate cell tracking systems;
- Video-conferencing systems;
- Firewalls and other security and networking technologies related to the above.

In addition to the development, implementation and maintenance of the above technologies, the team's scope also includes:

- Developing, in collaboration with program areas and the Governance Planning and Security division, related security policies, standards, procedures, disaster recovery plans and communications;
- Carrying out or overseeing regular maintenance on equipment
- Researching best practices and staying current with national trends
- Carrying out assessments of threats and risks related to facilities
- Responding to related emergency incidents and participating in post-incident analysis

The incumbent is an active member of the team providing the technical support for members of the Judiciary and their staff, ensuring timely response to operational matters affecting the delivery of court services. While the team is supported by professionals within the ISSS and the Technology Service Centre, they have the primary service relationship with the Judiciary and play a significant role in ensuring a high quality standard of service is maintained that reflects the unique requirements of the Judiciary and respects the independence of the Judicial Branch of the Government.

The position carries out its duties within a strict legislative and policy framework in accordance with Court Services and the Correctional Services Canada Acts, Regulations, Policies and Procedures, as well as various GNWT Acts and Regulations, such as the Financial Administration Act, Public Service Regulations and the Access to Information and Protection of Privacy Act.

The incumbent will be required to work closely with Judges, Directors, Wardens, facility managers, auditors, law enforcement, end users, vendors and other IMT staff. Duties must be carried out with a high degree of discipline and ethics, as the data being managed is often used in legal or disciplinary proceedings. The team is also required to travel to all territorial regions to work collaboratively with regional management, contractors and staff, as necessary.

The position will be required to work with technologies and information that have a direct impact on the health and well-being of individuals. Therefore, failure of any of the security systems would have a serious impact on the delivery of programs and services directed towards clients, the public and other stakeholders.

RESPONSIBILITIES

1. **Support the planning of security and operational technology solutions to support court services and specialized facility security requirements:**
   - Explains the purpose of and provides advice and guidance on the application and operation of physical, procedural and technical security controls.
   - Performs security risk, vulnerability assessments, and business impact analysis for medium complexity technology solutions. Investigates suspected attacks and manages security incidents. Uses forensics where appropriate.
   - Contributes to the creation and maintenance of policy, standards, procedures and documentation for security.

- Contributes to the availability management process and its operation and performs defined availability management tasks. Analyses service and component availability, reliability, maintainability and serviceability. Ensures that services and components meet and continue to meet all of their agreed performance targets and service levels. Implements arrangements for disaster recovery and documents recovery procedures. Conducts testing of recovery procedures.
- Supports monitoring of the external environment and assessment of emerging technologies to evaluate the potential impacts, threats and opportunities to the organisation. Contributes to the creation of reports, technology roadmapping and the sharing of knowledge and insights.
- Actively maintains knowledge in the technical specialty of facility security technologies. Provides detailed and specific advice regarding the application of this specialty to the organisation's planning and operations.

2. **Contributes to the design and implementation of technology enabled solutions supporting facility security and court services:**
   - Designs computing and communications solutions, taking account of target environment, performance, security and sustainability requirements. Translates logical designs into physical designs, and delivers technical prototypes of proposed components for approval by customer and execution by technicians.
   - Creates and executes test plans for systems and technology components. Records and analyses actions and results, and maintains a defect register.
   - Assesses and analyses release components. Provides input to scheduling. Ensures release processes and procedures are maintained.
   - Undertakes installations and de-installations of items of hardware and/or software. Takes action to ensure targets are met within established safety and quality procedures, including, where appropriate, handover to the client. Documents details of all hardware/software items that have been installed and removed so that configuration management records can be updated. Develops installation procedures and standards, and schedules installation work. Provides specialist guidance and advice to less experienced colleagues to ensure best use is made of available assets, and to maintain or improve the installation service.

3. **Operation and maintains equipment and solutions in support of court operations and facility security and monitoring systems:**
   - Applies tools, techniques and processes to create and maintain an accurate asset register. Produces reports and analysis to support asset management activities and aid decision making.
   - Carries out agreed operational procedures, including infrastructure configuration, installation, repair and maintenance.
   - Prioritizes and diagnoses incidents according to agreed procedures. Investigates causes of incidents and seeks resolution. Escalates unresolved incidents. Facilitates recovery, following resolution of incidents. Documents and closes resolved incidents according to agreed procedures.

- Monitors the application and compliance of security administration procedures and reviews information systems for actual or potential breaches in security. Ensures that all identified breaches in security are promptly and thoroughly investigated and that any system changes required to maintain security are implemented.
- Contributes to digital forensic investigations, working with law enforcement and corrections staff. Processes and analyses evidence in line with policy, standards and guidelines and supports production of forensics findings and reports.

WORKING CONDITIONS

Physical Demands

Work hours may be longer than usual or scheduled outside of normal working hours in order to minimize disruption. The incumbent will frequently be required to review work that has been conducted in tight spaces and, occasionally, be engaged in heavy physical and strenuous activities in hazardous circumstances that produce substantial discomfort. The incumbent will be required to travel to regional correctional facilities on an as-required basis. Travel within a one year period is expected to be approximately 3-4 weeks away from the office.

Environmental Conditions

During the required review and inspections of existing and any enhancement or replacement work, the incumbent will be exposed to extreme temperatures, loud environments and heights. Security device cables and wiring often run in crawlspaces and/or high ceilings; cameras are located both indoors and outdoors, some in areas that require man-lifts and/or specialized mobile jacks to reach the location. Inspections and the review of replacement work will expose the incumbent to these hazards. Within Correctional Facilities, precautions must also be taken against infectious diseases.

Sensory Demands

The incumbent is required to be attentive both visually and audibly while performing inspections, maintenance and tests of the security equipment.

Mental Demands

There are numerous tight deadlines and several complex projects that often occur concurrently.

KNOWLEDGE, SKILLS AND ABILITIES

- Advanced technical knowledge of facilities security systems and concepts.
- Broad experience and working knowledge of Information Technology (IT), Information Systems (IS) and Information Management (IM) concepts relating to security functionality and standards.
- Demonstrated knowledge of information technology service management (ITSM), particularly incident response and problem management. Knowledge of ITIL is an asset.
- Must have the ability to be an effective team member (with both staff and external contractors).

- Must have the ability to effectively manage time and respect preset timelines (the majority of security work conducted within the correctional facilities must be completed within pre-set windows of opportunity, delays can lead to restrictions in movement and the cancellation of rehabilitating program delivery).
- Proven experience with business continuity planning and disaster recovery planning.

Typically, the above qualifications would be attained by:

A University degree in either computer science or electrical engineering and three (3) years of directly related experience with facility security technologies.

ADDITIONAL REQUIREMENTS

Position Security (check one)

☐ 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: Select language

☐ Required
☐ Preferred