



IDENTIFICATION

Department	Position Title	
Finance	Manager, Justice Technical Services	
Position Number	Community	Division/Region
15-8175	Yellowknife	Information Systems Shared Services / HQ

PURPOSE OF THE POSITION

The Manager, Justice Technical Services is responsible for the overall planning, design, implementation, maintenance, and support of all electronic and physical security solutions used by the Department of Justice and the unique technology systems used to support Court Services, Correction Services, and Judiciary.

SCOPE

Located in Yellowknife, the Manager, Justice Technical Services reports to the Director of Information Systems Shared Services (ISSS) in the Department of Finance. Although the position resides within the Department of Finance, unique to this position is the requirement for a shared reporting relationship between the Director ISSS and the Judiciary of the NWT, where interests of both parties are independently represented and voiced depending on requirement. When representing the Judiciary, the position is referred to as “Chief Judicial Information/Security Officer” for the NWT Supreme Court and NWT Territorial Court.

The incumbent leads a technical team of four specialists. The team is responsible for the technology-enabled systems used by facilities operated by the Department of Justice, such as courthouses and correctional facilities. These include:

- Judiciary network services.
- 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 planning, design, implementation and maintenance of the above technology solutions, 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 and their team are the first point of contact 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 Information Systems Shared Services 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 Access to Information and Protection of Privacy Act.

The incumbent works closely with and influences 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. Travel to all territorial regions to work collaboratively with regional management, contractors and staff is required.

The position will make critical decisions that will have a direct impact on the health and wellbeing 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. Provide planning and advisory services related to technology enabled solutions to support Court operations and address specialized facility security needs:

- Provides advice and guidance on security strategies to manage identified risks and ensure adoption and adherence to standards. Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex technology solutions. Investigates major breaches of security and recommends appropriate control improvements.
- Develops standards, processes, and guidelines for ensuring the physical and electronic security of automated systems within a specific area. Ensures that the policy and standards for security administration are fit for purpose, current and correctly implemented.
- Provides advice, assistance and leadership associated with the planning, design and improvement of service and component availability, including the investigation of all breaches of availability targets and service non-availability, with the instigation of remedial activities. Plans arrangements for disaster recovery together with supporting processes and manages the testing of such plans.
- Monitors the external environment to gather intelligence on emerging technologies.
- Assesses and documents the impacts, threats, and opportunities to the organization.
- Creates reports and technology roadmaps and shares knowledge and insights with others.
- Actively maintains recognized expert level knowledge in the technical specialty of facility security technologies. Provides definitive and expert advice in this area.

2. Designs and implements technology enabled solutions.

- Specifies and designs complex hardware components/systems. Selects appropriate design standards, methods, and tools, consistent with agreed enterprise policies, and ensures they are applied effectively. Reviews others' designs to ensure selection of appropriate technology, efficient use of resources, and effective integration of multiple systems and technology. Ensures that hardware designs balance functional, service quality, security, systems management, and sustainability.
- Coordinates and manages planning of testing, including software security testing. Takes responsibility for integrity of testing and acceptance activities and coordinates the execution of these activities. Provides authoritative advice and guidance on any aspect of test planning and execution. Defines and communicates the test strategy for the project. Manages all test processes, including test plans, resources, costs, timescales, test



deliverables and traceability. Manages client relationships with respect to testing matters. Identifies process improvements and contributes to corporate testing standards and definition of best practice.

- Leads the assessment, analysis, planning and design of release packages, including assessment of risk. Liaises with business and IT partners on release scheduling and communication of progress. Conducts post release reviews. Ensures release processes and procedures are applied and that releases can be rolled back as needed. Identifies, evaluates, and manages the adoption of appropriate release and deployment tools, techniques, and processes.
- Takes responsibility for installation projects, providing effective team leadership, including information flow to and from the client during project work. Develops and implements quality plans and method statements. Monitors the effectiveness of installations and ensures that appropriate recommendation for change is made.

3. Oversees the operation and maintenance of technology enabled solutions in support of court operations and facility security and monitoring systems:

- Controls IT and related assts in one or more significant areas, ensuring that administration of the acquisition, storage, distribution, movement, and disposal of assets is carried out. Produces and analyses registers and histories of authorized assets (including, documentation, data, licenses and agreements for supply, warranty, and maintenance) and verifies that all these assets are in a known state and location.
- Ensures that incidents are handled according to agreed procedures. Investigates escalated incidents to responsible service owners and seeks resolution. Facilitates recovery, following resolution of incidents. Ensures that resolved incidents are properly documented and closed. Analyses causes of incidents and informs service owners to minimize probability of recurrence and contribute to service improvement. Analyses metrics and reports on performance of incident management process.
- Monitors the application and compliance of security administration procedures and reviews 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. Ensures that security records are accurate and complete and that requests for support are dealt with according to set standards and procedures.
- 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.



4. Manage team and professional relationships:

- Oversee the workload and professional development of team, ensuring skills remain up to date.
- Ensures team carries out duties with a commitment to ethics and compliance to policy.
- Maintain a culture and process of continuous service improvement.
- Maintain professional relationships with colleagues and stakeholders: Judges, Directors, Wardens, facility managers, auditors, law enforcement, end users, vendors, and other Information Management and Technology staff.
- Manage sourcing relationships with suppliers, ensuring appropriate sourcing and contracting arrangements, as well as quality and value for money.
- Stay informed of relevant legislation, regulations, advisories, alerts, and vulnerabilities, identifying issues and opportunities for GNWT.
- Manage relevant suppliers, including managing vendor performance, costs, contracts, and payments.
- Plan and monitor budgets and costs.

WORKING CONDITIONS

Physical Demands

Work hours may be longer than usual or scheduled outside of normal working hours 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.

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

No unusual demands.

Mental Demands

There are numerous tight deadlines and several complex projects that often occur concurrently. The incumbent will be required to travel to regional correctional facilities on an as-required-



basis. Travel within on-year period is expected to be approximately 3-4 weeks away from the office.

KNOWLEDGE, SKILLS, AND ABILITIES

- Knowledge of facilities, security systems and concepts.
- Experience and working knowledge of Information Technology (IT), Information Systems (IS) and Information Management (IM) concepts relating to security functionality and standards.
- Knowledge of information technology service management (ITSM), particularly incident response and problem management. Knowledge of ITIL is an asset.
- Must have the ability to manage others (both staff and external contractors).
- Must have the ability to manage time and respect preset timelines (most 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).
- Understanding of risk management concepts and techniques (such as ISO 31000) and the ability to formulate recommendations for control improvements to senior management.
- Experience with business continuity planning, disaster recovery planning, redundancy or failover of equipment expertise, contingency planning, and emergency support.
- Experience in electronics and the functionality of state-of-the-art security systems.
- Experience with procurement, contracting, vendor management and contract negotiation.
- 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 Completion of an undergraduate degree in computer science or electrical engineering with five (5) or more years of directly relevant and progressive experience including one (1) year supervising staff.

Equivalent combinations of education and experience will be considered.

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