Government of
Northwest Territories

IDENTIFICATION

Department	Position Title	
Finance	Chief Information Security Officer	
Position Number	**Community**	**Division/Region**
15-12298	Yellowknife	Governance, Planning and Security

PURPOSE OF THE POSITION

The Chief Information Security Officer (CISO) is responsible for the selection, design, justification, implementation and oversight of operational controls and management strategies to maintain confidentiality, integrity, availability of information and compliance of information systems with legislation, regulation, and relevant policies and standards.

As the GNWT's technology landscape becomes more complex and distributed the potential exposure to internal and external threats, unintended risks or dedicated attacks on the government's assets and information increases. The Chief Information Security Officer will use security frameworks and other best practises to effectively and efficiently reduce business risks and ensuring our I&T service providers are in compliance with GNWT security standards.

SCOPE

The Chief Information Security Officer is located in Yellowknife and reports to the Director of the Governance, Planning and Security division within the Information Systems Shared Service activity in the Department of Finance.

The position is responsible for development and communication of enterprise-wide information security policy, directives, standards and guidelines, and contributes to the development of organizational strategies that address information control requirements.

A significant portion of the job is providing assurance to senior management on the protection of integrity, availability, authenticity, non-repudiation and confidentiality of information and the management of risk in a pragmatic and cost effective manner to ensure stakeholder confidence.

The CISO provides expert level policy and security planning services to; management and staff within the information and technology (I&T) sector in government, senior management government-wide, the Government Chief Information Officer, and Deputy Heads via the Informatics Policy Council (IPC).

The CISO is a change agent who collaboratively develops and communicates security controls within the I&T sector with program stakeholders. The position develops and contributes to corporate approaches, such as an integrated approach to identity management. The position provides input into broader strategies that align with, complement or build on strategic initiatives.

The CISO leads a team of Security Analysts that work collaboratively with stakeholders government-wide, including Departments, Boards & Agencies. The incumbent will typically liaise with senior management with program accountabilities, as well as I&T sector management and will work with external contractors and vendors, as needed.

The CISO needs to be fully familiar with recognized security bodies of knowledge both generic and specific, they must also actively seek out new knowledge for own personal development and the mentoring or coaching of others.

The incumbent participates in internal and external teams, committees, programs and projects, representing the GNWT on Federal/Provincial/Territorial (F/P/T) groups including the National CIO Sub-Committee on Information Systems Protection (NCSIP), a sub-committee of the Public Sector CIO Council (PSCIOC) and the F/P/T group responsible for Cyber Security and supports the Deputy Minister of Justice in his/her role on the F/P /T DMs of Cyber Security table.

This position works within a Legislative and Policy framework and carries out its responsibilities in accordance with GNWT acts, regulations, policies and procedures that include such things as the Access to Information and Protection of Privacy Act, Financial Administration Act, and various government policies.

RESPONSIBILITIES

1. **Develops and leads implementation of security strategies and policy tools, to ensure adoption and adherence to standards, and appropriate documentation to meet GNWT auditing, reporting and compliance requirements.**
   - Drives adoption of and adherence to policies and standards through the provision of expert advice and guidance in order to ensure architectural principles are applied, requirements are defined and rigorous security testing is applied;
   - Oversee, monitor, communicate and report on the implementation and adoption of information security policy, standards, exceptions, risk assessments and awareness efforts;
   - Develop and maintain, in collaboration with the GNWT Access & Privacy Office and I&T management and staff, a government-wide security program (including awareness)

and initiatives that address identified risks and business information security requirements;
- Identifies and monitors environmental and market trends and pro-actively assesses impact on business strategies, benefits and risks;
- Chair and participate on inter-departmental and inter-jurisdictional security committees;
- Communicate the state of security to senior management and solicit involvement in achieving higher levels of security through information sharing and co-operation.

2. **Provides advice, guidance and expertise to promote the adoption of information security management methods and tools and applies these to manage risks.**
   - Evaluates and selects appropriate methods and tools that align with agreed standards and guidelines;
   - Oversees the implementation of the methods and tools at the programme, project and team level;
   - Negotiate and manage contracts and service agreements with solution vendors and service providers/contractors for security-related products and services;
   - Consult with I&T sector staff to ensure that security is factored into the evaluation, selection, installation and configuration of infrastructure and applications.

3. **Provides operational services and support to the I&T sector and department leadership teams.**
   - Obtains and acts on vulnerability information and conducts security risk assessments, business impact analysis and accreditation on complex information systems;
   - Manage security incident response framework and oversee implementation of response/mitigation measures.
   - Investigates major breaches of security and recommends appropriate control improvements;
   - Lead incident handling activities within the GNWT to ensure incident response is appropriate and effective, including developing the network, providing training, tools, guidance and incident reports, as needed.
   - Consult with senior managers during information security incidents to ensure the situation is managed properly, recommending appropriate action, and reporting regularly on the status of security issues and progress;
   - Oversee and manage vulnerability audits and assessments;
   - Leads the GNWT I&T Sector Risk Council to ensure an integrated, coordinated approach to Risk leadership. This involves Council (network) development, identification, prioritization, assignment and monitoring of risks. The Risk Council reports to the I&T Sector Leaders.
   - Assist resource owners and I&T staff in understanding and responding to audits;
   - Ensure audit trails, system logs and other monitoring data sources are reviewed periodically and are in compliance with policies and audit requirements;
   - Design, coordinate and oversee security testing to verify security of systems, networks & applications, and manage the remediation of identified risks;

- Maintain a knowledgebase comprising a technical reference library, security advisories and alerts, security trends and practices, and laws and regulations;
- Work with I&T and business stakeholders to classify data and systems and define metrics and reporting strategies to communicate progress;
- Coordinate and oversee security-related activities with all I&T service teams, including the Technology Services Centre, Application services and 3rd party providers.

4. **Manages the planning and human resources work for the information security unit.**
   - Delegates responsibilities as appropriate. Sets performance targets, and monitors progress against agreed quality and performance criteria.
   - Provides effective feedback, throughout the performance management cycle, to ensure optimum performance.
   - Proactively works to ensure effective working relationships within the team and with those whom the team interacts with.
   - Encourages pro-active development of skills and capabilities and provides mentoring to support professional development.
   - Provides input in to formal processes such as job description development and disciplinary procedures.
   - Provides training to team through internal cross training and external sources.
   - Monitors security resources and service demands on team.

5. **Contributes to the financial planning of the Division and other projects.**
   - Develop short and long term budget projections, business cases, funding submissions and identify and advocate for resources to support security initiatives;
   - Assists with the definition and operation of effective financial control and decision making, especially in the areas of information security, cyber security and technology operational controls.
   - Analyses actual expenditure, explains variances, and advises on options in use of available budget.
   - Manage procurement process for security solutions, working with I&T stakeholders.

WORKING CONDITIONS

Physical Demands

No unusual demands.

Environmental Conditions

No unusual demands.

Sensory Demands

The incumbent is required to be very attentive both visually and audibly while managing and monitoring security incidents. Accuracy is crucial in this position, particularly when making decisions and providing reports to external stakeholders. The incumbent will need to have excellent attention to detail throughout the course of each work day.

Mental Demands

During a security crisis there is potential for mental, physical and emotional fatigue and stress. The CISO is seen as the subject matter expert whose scope of work can involve politically sensitive and legal issues with tight deadlines for resolution/answers and a high degree of intensity. High levels of concentration and attention are essential.

Ongoing learning is required. The complexity of the environment and the challenge of keeping current with evolving security technology requires time, energy and skill to do competently with due diligence. Incumbent may experience some stress due to nature of the position and the reporting expectations - to GNWT Senior management and I&T sector with varying information reporting preferences. A disruption in lifestyle may be caused by work schedules or travel requirements.

KNOWLEDGE, SKILLS AND ABILITIES

- Expert ability to assess, evaluate and manage risk, leveraging industry standards like those from ISACA or the Industry Standards Organization (ISO).
- Expert knowledge and understanding of industry-specific standards and methodologies including information security management frameworks such as International Standards Organization (ISO) 27001, 27002, the IT Infrastructure Library (ITIL) and COBIT.
- Current understanding/knowledge of the IT security industry, including best practices, solution awareness, security processes and new attacks and threats.
- Demonstrated current and conceptual understanding of the government Enterprise Risk Management (ERM) framework and how to apply that framework.
- Good understanding of applicable legal and regulatory requirements including, but not limited to the *Financial Administration Act*, Financial Administration Manual, Contracting & Procurement Regulations, *Public Service Act*, Public Service Regulations, and the *Access to Information and Protection of Privacy Act*.
- Strong analytical skills to analyze security requirements and relate them to appropriate security controls.
- Demonstrated experience in system and application technology security testing (vulnerability scanning and penetration testing, white box, black box and code review).
- Ability to develop and maintain policies, procedures, standards and guidelines and working with legal, audit and compliance functions.
- Effective written and verbal communications skills, including the ability to maintain professional communications in difficult circumstances; articulate and persuasive communicator and negotiator.
- Able to translate technical language to a non-technical audience
- Ability to write investment proposals, such as business cases.
- Strong leadership and team building skills.
- Good change management and change leadership skills.
- Able to manage both the supply and demand for services.
- Able to lead calmly during times of stress.
- Able to work with a high degree of independence.

- Good administrative, coordinating and delegation abilities.
- Good interpersonal skills, exercising significant tact and discretion.
- Demonstrated experience partnering and collaborating at multiple organizational levels.
- Good working knowledge of government processes, including business planning, main estimates, forced growth, capital planning, and FMB and Cabinet decision-making processes.
- Strong business and technical background to work with the IT and business organizations to align security priorities and plans with business objectives.
- Ability to prioritize work, balance strategic and operational security efforts.
- Demonstrated strategic-thinking, sound judgment & practical problem-solving skills.
- Demonstrates leadership, communicates effectively, both formally and informally, and facilitates collaboration between stakeholders who have diverse objectives. This incumbent leads the security culture of the organization.

Typically, the above qualifications would be attained by:

Completion of an undergraduate degree in computer science or management information systems with a focus on security technologies, with at least 6 years IT experience, including a minimum of 2 years of direct experience leading an Information Security program, and 2 years managing staff and budgets.
Desired professional certifications include:

- Certified Information Systems Security Professional (CISSP) and either a Certified Information Systems Auditor (CISA) or Certified Manager of Information Security (CISM) designation. Other combinations and/or certifications may 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

CERTIFICATION

Title: Chief Information Security Officer

Position Number: 15-12298

Employee Signature	Supervisor Signature
Printed Name	Printed Name
Date	Date
I certify that I have read and understand the responsibilities assigned to this position.	*I certify that this job description is an accurate description of the responsibilities assigned to the position.*
Deputy Head/Delegate Signature	Date
I approve the delegation of the responsibilities outlined herein within the context of the attached organizational structure.	

The above statements are intended to describe the general nature and level of work being performed by the incumbents of this job. They are not intended to be an exhaustive list of all responsibilities and activities required of this position.