Northwest Territories Finance

## IDENTIFICATION

| *Position Number* | *Position Title* | |
|---|---|---|
| 15-13956 | Information Security Analyst | |
| ***Department*** | ***Division/Region*** | ***Location*** |
| Finance | Office of the Chief Information Officer | Yellowknife |

## PURPOSE OF THE POSITION

The Information Security Analyst performs two core functions for the Government of Northwest Territories. The first is the development and maintenance of information security policies, procedures, standards and guidelines for use throughout the GNWT. The second function is to apply those to the infrastructure and applications of the GNWT through a variety of means.

## SCOPE

Located in Yellowknife, the incumbent will work within the Office of the Chief Information Officer (OCIO), reporting to the Manager of Information Security. As a corporate function, the scope of the OCIO regarding information security includes all the data, infrastructure and software/applications throughout the GNWT. 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 government information security, and consulting with departments to understand their business functions and interpret their appetite and tolerance for risk and translate that into an actionable desired future state.

The incumbent will not work directly hands on implementing security measures on the infrastructure or applications but will work closely with the departmental 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 best practices to ensure the most effective implementation of information security measures and practices.

Compared to the *Junior* Information Security Analyst, the Information Security Analyst will be assigned to more difficult tasks, in terms of political sensitivity, technical complexity, urgency, etc... The Information Security Analyst will be expected to use their greater experience and judgment to provide review, coaching, guidance and advice to the junior position.

## RESPONSIBILITIES

- 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.
- Participate 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 Network Architect in the Technology Services Centre (TSC) to ensure the security of GNWT technology infrastructure.
- Assist in 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 departments 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 particular systems. This may be done in coordination with an external professional security services firm or consultant.
- Deliver, or work with the Manager of Information Security and/or a consultant to deliver, information security training and awareness programs throughout the GNWT.
- Collaborate with other Canadian jurisdictions to benchmark the security measures of the GNWT against other governments.

## 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.
- Familiarity with systems development life cycles (SDLC) and the integration of information security best practices within a SDLC.
- Experience with common protocols such as TCP/IP, SNMP, HTTP, Radius and broad understanding of cryptography technologies/protocols including Kerberos, PKI, and AES/DES.
- Relevant industry certifications (*i.e.* CISSP, CISA, CISM, SANS, *etc...*).
- Knowledge of information security and privacy legislation in a Canadian context.

- High level of analytical and problem solving abilities.
- Ability to conduct research into security issues and products, as required.
- Excellent interpersonal, communication and organizational skills. Excellent attention to detail.
- Ability to negotiate, persuade and find compromise between stakeholders.
- Ability to develop oneself professionally to meet the growing security needs of the GNWT.
- Ability to remain calm and focused during difficult situations.

## TYPICALLY, THE ABOVE QUALIFICATIONS WOULD BE ATTAINED BY:

- Completion of a college or university degree in a related Engineering, Computer Science, Information Systems or Information Management program; and
- Six (6) years working in the field of Information Technology,
    - Three (3) of those years being within the field of Information Security.

Additional current industry-standard certifications in the IT security field will be recognized as part of the education/training component of the requirements for this position.

## WORKING CONDITIONS

### Physical Demands

Are consistent with the typical GNWT office environment while working. Heavy lifting as well as crawling in awkward spaces are required as part of implementation and maintenance activities.

### Environmental Conditions

Are consistent with the typical GNWT office environment while working in the office.

### Mental Demands

The incumbent will be working in a technology environment where he or she is seen as an expert on security by peers who have some security expertise too and this calls for confidence, and ability to diagnose security problems right the first time. This may place some stress to people who have never done consulting where they are seen as experts. Security incidents may cause intermittent high stress situations.

## ADDITIONAL REQUIREMENTS

**Position Security** (check one)

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

## EXCLUSION/INCLUSION

### Section A

☒This job should be included in the bargaining unit

☐This job should be excluded from the bargaining unit (complete section B)

### Section B – Rationale for exclusion from the bargaining unit

(Exclusion from the bargaining unit must meet the conditions outlined in section 306 of the GNWT's Human Resources Manual (HRM). Refer to Section 306 of the GNWT's HRM and outline the reason for the exclusion request below)

Comments: Not Applicable.

I approve the delegation of the responsibilities outlined herein within the context of the attached organizational structure.