IDENTIFICATION

Department	Position Title	
Finance	Manager, Cybersecurity Operations	
Position Number	**Community**	**Division/Region**
15-17772	Yellowknife	Technology Service Centre

PURPOSE OF THE POSITION

The Manager, Cybersecurity Operations is a pivotal role within the Government of the Northwest Territories (GNWT), responsible for overseeing the security management and operations of GNWT's IT infrastructure and safeguarding sensitive information. This role ensures effective monitoring, detection, response, and mitigation of cybersecurity threats across on-premises, cloud, and hybrid environments. The incumbent will build and lead a team of cybersecurity analysts, contribute to strategic security initiatives developed by the Chief Information Security Officer (CISO), manage cybersecurity vendors, provide incident preparedness, detection and response support, to ensure the continuity and resilience of GNWT's IT operations. This position is critical in protecting GNWT's information holdings, maintaining public trust in GNWT services, and ensuring compliance with established policies.

SCOPE

The Manager, Cybersecurity Operations is based in Yellowknife, Northwest Territories, and reports to the Director, Technology Services Centre. The Manager will lead a team of cybersecurity Operations (SecOps) analysts, provide leadership and ensure alignment with GNWT's strategic objectives. The role includes managing a designated cybersecurity operations budget, overseeing Managed Security Services (MSS) contracts, and ensuring effective use of resources to enhance the organization's security posture in collaboration with the CISO.

The Manager is tasked with safeguarding GNWT's information technology infrastructure and systems and ensuring compliance with regulatory and security standards. This involves overseeing the monitoring and protection of both on-premises and cloud-based systems, coordinating incident responses, conducting security threat and risk assessments on IT infrastructure and systems, and fostering collaboration across departments to maintain the integrity of IT operations. The scope of this position covers the entire GNWT enterprise suite of applications and infrastructure irrespective of IT provider or responsible departments, board

or agencies. By addressing current and emerging threats, the role supports the GNWT's mission to deliver secure and reliable services to the public.

Through proactive planning, effective team management and vendor oversight, this position connects the technical and operational responsibilities of cybersecurity with broader organizational goals. The role conducts regular operational vulnerability assessments and provides operational security training to IT employees. This integrated approach ensures GNWT is resilient against cybersecurity risks and capable of responding swiftly to incidents.

The Manager, Cybersecurity Operations works closely with the Chief Information Security Officer (CISO) to ensure operational activities align with GNWT's enterprise security strategy. The CISO contributes to the Manager's workplan by identifying strategic priorities, supporting incident coordination, and providing oversight to ensure work is completed in accordance with GNWT policies, standards, and risk frameworks.

RESPONSIBILITIES

1. **Lead and manage GNWT's cybersecurity operations to ensure effective protection of IT** infrastructure and systems.
   - Oversee day-to-day cybersecurity operations including monitoring, alerting, and incident triage.
   - Manage the contract, performance and service delivery of GNWT's Managed Security Service Provider (MSSP) in consultation with the CISO.
   - Ensure operational alignment with GNWT security policies and standards.

2. **Coordinate and execute incident detection, and response activities across GNWT's I&T environment.**
   - Lead technical response efforts for cybersecurity incidents, including detection, containment and recovery.
   - Collaborate with internal teams and external partners during incident investigations.
   - Conduct training and exercises, establish clear communication protocols, and assign specific roles and responsibilities to individuals and teams.

3. **Manage vulnerability and threat detection programs to reduce GNWT's exposure to cyber risks.**
   - Conduct regular vulnerability scans and coordinate remediation efforts.
   - Monitor threat intelligence feeds and ensure timely response to emerging threats.
   - Track and report on risk mitigation activities.

4. **Administer and optimize GNWT's security infrastructure and tools.**
   - Operate and maintain security platforms such as SIEM and endpoint protection.
   - Ensure logging, alerting, and monitoring systems are functioning effectively.
   - Recommend improvements to enhance security posture and operational efficiency.

5. **Provide operational reporting and metrics to support compliance and decision-making.**
   - Track and report key performance indicators such as mean time to detect (MTTD), meant time to respond (MTTR), vulnerability remediation rates, SLA compliance for the MSSP, and threat trends.
   - Support audit and compliance activities by providing operational data and documentation.
   - Contribute to the development of business cases and funding submissions for security initiatives.

6. **Collaborate with internal and external stakeholders to implement security controls and initiatives.**
   - Work closely with IT teams (endpoint, infrastructure, applications) to integrate a security first mindset into operations.
   - Support CISO-led initiatives by providing operational insights and execution support.
   - Participate in cross-functional projects and working groups related to cybersecurity.

7. **Leadership and Training**
   - Lead and manage a team of cybersecurity analysts.
   - Deliver regular training to enhance the team's expertise.
   - Foster a collaborative team environment.

WORKING CONDITIONS

Physical Demands

No unusual demands

Environmental Conditions

No unusual demands

Sensory Demands

No unusual demands

Mental Demands

Availability for on-call duties required for critical incidents. Requires managing complex issues and communicating effectively with diverse audiences. Requires occasional travel away from home.

KNOWLEDGE, SKILLS AND ABILITIES

- Technical knowledge of cybersecurity tools and platforms (e.g., SIEM, IDS/IPS, endpoint protection).
- Understanding of cloud security principles (AWS, Azure, GCP) and tools.
- Knowledge of MSSPs or third-party security service providers.
- Knowledge of government IT environments and service delivery models.
- Knowledge of reporting and performance metrics.
- Proficiency in incident response, threat detection, and vulnerability management.
- Ability to interpret and apply security policies, standards, and frameworks (e.g., ISO 27001, NIST).
- Analytical and problem-solving skills.
- Communication skills, including the ability to translate technical issues for non-technical audiences.
- Organizational and time management skills.
- Ability to lead teams (including mixed teams with vendors) and manage operational priorities under pressure.
- Ability to build and maintain collaborative working relationships.
- Ability to manage budgets and contracts.
- Ability to mentor and develop high-performing teams.
- Ability to manage competing priorities in a dynamic environment.
- 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 Bachelor's degree in Computer Science, Information Security, Cybersecurity, or a related field and 5 years of experience in cybersecurity operations or IT security, including experience with IT Infrastructure (Networking, Identity Management, Active Directory, Microsoft 365, Azure security) and endpoint security, including 1 year of experience in a managerial or team leadership role involving IT audit, risk management, incident response, or security operations.

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