GOVERNMENT COMMUNICATIONS SECURITY BUREAU
TE TIRA TIAKI

# POSITION DESCRIPTION

## Manager, Cyber Threat Response

**Unit/Branch, Directorate:** Information Assurance & Cyber Security (IACD)

**Location:** Wellington

**Salary range:** J $106,860 - $160,290

---

**Purpose of position:** The Manager for Cyber Threat Response (CTR) is responsible for the oversight and management of the National Cyber Security Centre's reporting output and incident handling functions. The CTR Manager is responsible for leading teams of Incident Responders, Incident Coordinators and Cyber Threat Analysts, who in turn, analyse, evaluate, respond to, and report cyber security threats. The Manager works to ensure that the unit retains enhanced analytic capabilities and forensic investigation tradecraft.

---

**Our mission** at the GCSB is to protect and enhance New Zealand's security and wellbeing.

**Our values** are Respect, Commitment, Integrity and Courage.

---

**Information Assurance and Cyber Security Directorate purpose:** The IAC Directorate contributes to the national security of New Zealand by providing technical advice and assistance to Government and organisations with significant national information infrastructures to enable them to protect their information from advanced technology-borne threats. To achieve this, the Directorate provides technical security inspections; high-grade encryption services; information assurance policy and advice; regulation of telecommunications & space activities; and high-end cyber security services to detect and respond to such threats. The National Cyber Security Centre (NCSC) is part of the IAC Directorate.

| Key accountabilities | Deliverables/Outcomes |
|---|---|
| **Promoting cross-team collaboration through the execution of the IACD Strategic Plan and support for operational exchanges between different IACD business units.**<br>• Participating in both functional (specific skill-sets) and cross-functional (mixed skill-sets) IACD teams at the request of the IACD Executive Team and Leadership Group.<br>• Pro-actively demonstrating a willingness to transfer skill sets to other teams in times of operational surge and crisis.<br>• Making a constructive contribution to the execution of the Strategic Plan. | • Team silos are visibly reduced and the focus of staff shifts from their own unit plan to delivering Directorate-wide objectives.<br>• Customer feedback suggests that the plan is having a positive effect on IACD's performance through the creation of a more obviously joined-up operating model.<br>• Policy and process gaps, which negatively affect IACD operations, are highlighted and rectified.<br>• Staff retain an active interest in developments within IACD beyond their normal area of operation. |
| **Developing and Managing People**<br>• Effectively lead, develop and manage unit staff and positively influence their progress towards successful results.<br>• Effectively manage workloads to ensure they are appropriate to meet Unit objectives and staff abilities.<br>• In conjunction with People Capability, address poor performance of employees and ensure that good conduct and discipline is maintained at all times and any issues are dealt with promptly.<br>• Demonstrate the stated values of the organisation in all aspects of their representation of the team/Bureau.<br>• Ensure performance objectives, reviews and discussions are completed in line with Bureau policies and procedures for all direct reports.<br>• Conduct regular team meetings to share information and update staff on new requirements and policies.<br>• Support supervisors and team leaders to achieve objectives, identify personal development opportunities, recognise areas of improvement and establish solution based outcomes.<br>• Ensure effective recruitment to attract the best person for the position and then ensure a complete and comprehensive induction takes place.<br>• Ensure a training program is designed and implemented for all staff. | • Staff are motivated and engaged with a clear understanding of the technical requirements that meet unit and organisational objectives.<br>• Staff and unit workloads are managed to ensure:<br>  ○ Unit priorities are and outcomes are met<br>  ○ Staff are fully employed commensurate with their individual level<br>  ○ Unit and staff performance is continuously monitored with any variance addressed fairly and within an appropriate timeframe<br>  ○ Organisational values are represented appropriately and respectfully.<br>  ○ Performance management obligations are completed within published schedules.<br>  ○ Recommendations for improvement and staff development opportunities are considered<br>• The Unit is kept appraised on a regular basis with clear and open sharing of appropriate information.<br>• Supervisory and other leadership staff are developed with succession in mind and to ensure the continued stability and success of the Unit.<br>• Appropriate staff are recruited with induction obligations met and signed off.<br>• Staff are appropriately trained to meet Unit |

| | |
|---|---|
| | objectives.<br>• Unit is performing to its expected potential. |
| **Business and Financial Planning**<br>• Work with the IACD Business Manager to manage and maintain the Unit's annual budget in accordance with GCSB Finance Instructions. Report monthly on any variances to the Finance business unit.<br>• Unit business plans are developed to enhance the capability and outputs of the Unit.<br>• Unit business plans are clearly communicated to the team and inform individual performance objectives.<br>• Contribute to the management and planning for the NCSC. | • Unit financial obligations are met within GCSB financial instructions and the Budget spent in accordance with financial authority.<br>• Unit business plans are developed, monitored, and adjusted to ensure unit meets GCSB expectations.<br>• Business growth opportunities are identified, evaluated, and recommended appropriately.<br>• Supervisors, team leaders and staff understand how their work and outputs contribute to the Business Plan.<br>• Business Plan objectives are reflected in all individual performance plans.<br>• Unit objectives compliment NCSC objectives, and the NCSC operates as a cohesive whole. |
| **Delivery of Output**<br>• Ensure that Unit output effectively meets customer requirements and is of the highest quality.<br>• Manage and monitor the preparation and documentation of operational risk and threat assessments, as well as investigative options and plans.<br>• Manage and monitor the collection, analysis, and assimilation of all-source data, investigative leads and forensic evidence. Ensure that exhibit handling and documentation is conducted in accordance with forensic principles and GCSB Policy.<br>• Ensure all unit members understand and comply with their legal and compliance obligations. Develop and build a culture of compliance within in IACD.<br>• Manage and monitor the integrity and validity of CND reporting, investigative conclusions and assessments.<br>• Manage and monitor the provision of technical answers to questions regarding the compromise of New Zealand victim networks.<br>• Manage and monitor the development and understanding of mitigation design, advice and consequences.<br>• Manage personal operational tasking, and | • Operational threats and risks are correctly identified and documented, and actively managed throughout an investigation.<br>• Investigation plans and outcomes are appropriately documented and signed off prior to deployment and/or action.<br>• Legal authorities are understood across the Unit, and sought through appropriate mechanisms as required.<br>• Investigative leads are appropriately aggregated, understood, and evaluated to ensure correct investigative conclusions. Exhibits are correctly handled and recorded with full audit capabilities.<br>• Operations are managed against agreed deliverables.<br>• The content of investigative reporting and mitigation advice is unambiguous in its meaning, and implications of why it is being provided are clear.<br>• Investigative conclusions and assessments are valid and justifiable, and meet peer-review expectations.<br>• Output is correctly prioritised to maximise customer and GCSB value.<br>• Briefings and reports are appropriately constructed and delivered to ensure that a consistent and accurate message is delivered to all stakeholders. |

| | |
|---|---|
| remain aware of unit-wide operational developments, to ensure timeliness and deliverables.<br>• Support the lead Technical Lead for Incident Coordination and Response in managing and maintaining operational cover provisions.<br>• Manage and monitor operational briefings.<br>• Manage and monitor the Unit's engineering and research activities. | • Research and development projects support Unit business plans. |
| **Customer & Partner Liaison**<br>• Enhance GCSB's relationships and reputation with customers and partners through professionalism, representation and engagement.<br>• Develop and manage a range of relationships, at both a domestic and international level. Seek out and develop new customer and operational relationships, to further enhance the team's capabilities and reputation.<br>• Provide technical leadership and advice to customer, partner, and other entities.<br>• Ensure that output capabilities and limitations are known to customers where appropriate. Assist customers in understanding the correct mechanisms for tasking the section, and ensure that outputs are tailored to meet customer needs.<br>• Monitor business and external drivers, and technology trends that are likely to impact GCSB business and stakeholders. | • Productive and enduring relationships are formed with domestic and international partners.<br>• Customers (victims) are positively engaged in the investigative process, and are kept appropriately informed of investigative findings. Customer concerns and expectations are appropriately managed.<br>• GCSB is kept advised of external factors that may influence strategic direction of the Incident Coordination and Response and other units. |

| | |
|---|---|
| **Health and safety (for self)**<br>• Work safely and take responsibility for keeping self and colleagues free from harm.<br>• Report all incidents and hazards promptly.<br>• Know what to do in the event of an emergency.<br>• Cooperate in implementing return to work plans.<br>• Be a **visible** role model at all times.<br>• **Follow** GCSB's safety rules and procedures.<br><br>**Health and safety (for team):**<br>• Inform, train and equip staff to carry out their work safely.<br>• Ensure prompt and accurate reporting and investigation of all workplace incidents and injuries.<br>• Assess all hazards promptly and ensure they are managed. | • A safe and healthy workplace for all people using our sites as a place of work.<br>• All requirements in the NZIC Health and Safety policy and procedures are met. |
| Other duties | Any other duties that fall within the scope of the position. |

| **Position delegation** | |
|---|---|
| Financial delegation: | Level 4 |

| **Key stakeholders** | |
|---|---|
| Internal: | • Information Assurance and Cyber Security staff.<br>• GCSB IT Security staff.<br>• GCSB Intelligence staff.<br>• Other GCSB Staff as necessary. |
| External: | • NZ Government Agencies.<br>• NZSIS Investigations staff and State Intelligence Analysts.<br>• National Cyber Policy Office staff.<br>• Organisations of national significance.<br>• Cyber Security partner organisations.<br>• Victim organisations. |

| Person Specification | |
|---|---|
| Experience: | • Experience at a management level in the use of human, technical, and financial resources.<br>• Experience in the development and management of policy and plans at a corporate level.<br>• Experience in leading and managing a team of technical professionals.<br>• Extensive operational experience in the application of information assurance or security techniques and countermeasures.<br>• At least 5 years' experience in IT security or network defence, is desirable. |
| Knowledge and Skills: | • Highly developed communication, negotiation and relationship management skills.<br>• The ability to identify and resolve highly complex issues in an environment where there may be little or no prior guidance.<br>• The ability to conceptualise and develop innovative solutions.<br>• Good understanding of the IT security industry and the machinery of government, is desirable. |
| Qualifications and Courses: | • Tertiary degree, or equivalent experience, in Computer Science, Computer Forensics, or Computer Security.<br>• Completion of industry-recognised training in Incident handling or Forensic Analysis, is desirable. |
| Specific Job Requirements: | • Ability to obtain and maintain a TSS security clearance. |

## NZIC Competencies

In addition to the Person Specification above, competency standards which outline the development requirements of the position are set out under the NZ Intelligence Community (NZIC) Career Pathways framework. The Career Pathways framework enables progression within the job.

Full descriptions of progression competencies and an overview of the NZIC Career Pathways framework is available on appointment.

## Changes to Position Description

Positions in the GCSB may change over time as the organisation develops. Therefore we are committed to maintaining a flexible organisation structure that best enables us to meet changing market and customer needs. Responsibilities for this position may change over time as the job evolves. This Position Description may be reviewed as part of planning for the annual performance cycle.

Date PD reviewed: 13/09/2018

| Signatures | | |
|---|---|---|
| Manager's Name | | |
| Signature | | Date: |

| | | |
|---|---|---|
| Employee's Name | | |
| Signature | | Date: |