New Zealand Intelligence Community
Te Rōpū Pārongo Tārehu o Aotearoa
nzic.govt.nz

Position Description

Team Leader, Engagement Management

Business unit:	Outreach & Engagement Information Assurance and Cyber Security (IAC) Directorate
Position purpose:	Manage the team providing cyber security services, liaison and outreach assistance to New Zealand Government agencies and to Critical National Infrastructure (CNI) owners and operators in both public and private sectors.
Financial delegation:	Nil
Directorate overview:	The IAC Directorate contributes to the national security of New Zealand by providing 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 high assurance services; information assurance policy and advice; and high-end cyber security services to detect and respond to such threats.
Business Unit Overview	The Outreach and Engagement unit is responsible for the promotion of good practice information security policy and practice in New Zealand. The unit plays the lead for representational and external relationship building for the NCSC. Its team of Engagement Managers engage Government and significant national organisations to provide a touch point to the GCSB and NCSC in order to facilitate the delivery of information assurance and cyber security services.
Remuneration indicator:	Band I

Date evaluated	July 2014

GCSB vision and values

Our vision

Protecting and Enhancing New Zealand's Security and Wellbeing.

Our values

Respect, Commitment, Integrity, Courage.

Information Assurance & Cyber security Directorate vision, mission and goal

Our vision

"*Protect New Zealand's vital information infrastructures"*

Our mission

To be a team of confident professionals, admired for our innovation and regarded both domestically and internationally as leaders in the Information Assurance and Cyber sectors.
To have a comprehensive understanding of the advanced, technology-borne attempts to target our vital information infrastructures and steal our secrets and intellectual property.
To be confident about our ability to monitor these threats and either reduce harm directly through timely provision of assurance and technical services or help others to mitigate risks through authoritative policy and expert advice built on our unique capabilities.

Our goal

Impenetrable infrastructure: New Zealand's most important information infrastructures are impenetrable to technology borne compromise.

Role specification

Functional Relationships

External	Internal
■ NZ Government agencies ■ NZ significant national organisations ■ International cyber security centres, cryptologic agencies, technical security and critical infrastructure protection agencies. ■ Key partner agencies. ■ As necessary, other private or commercial organisations with cyber security interests	■ Outreach and Engagement Management staff ■ NCSC units ■ Directorate staff ■ GCSB mission enablement staff

Key result areas

The position of Team Leader, Engagement Management encompasses the following major functions or Key Result Areas:

- Contribute to the execution of the IACD Operational Plan
- Leadership, development and management of team members
- Coordination of Cyber Security consultancy services and related Information Assurance (IA)
- Liaison with international and domestic partner agencies, IT security community and industry

The requirements in the above Key Result Areas are broadly identified below:

Jobholder is accountable for:	Jobholder is successful when:
<u>Contribute to the execution of the IACD Operational Plan</u> ■ Promoting cross-team collaboration through the execution of the IACD Operational Plan and support for operational exchanges between different IACD business units ■ 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. ■ Pro-actively demonstrating a willingness	■ Team silos are visibly reduced and the focus of staff shifts from their own unit plan to delivering Directorate-wide objectives. ■ 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; ■ Policy and process gaps, which negatively affect IACD operations, are highlighted and rectified. ■ Staff retain an active interest in

to transfer skill sets to other teams in times of operational surge and crisis. ■ Making a constructive contribution to the execution of the Operational Plan.	developments within IACD beyond their normal area of operation. ■ Specific measure: active participation in at least one Operational Plan Working Group; a positive response to Senior Leadership requests for assistance beyond day-to-day responsibilities.
Leadership, development and management of team members ■ Day to day leadership of the team to positively influence progress towards successful results ■ Effectively manage workloads to ensure they are equitable ■ In conjunction with the Unit Manager, Outreach & Engagement, address poor performance of employees and ensure that good conduct and discipline is maintained at all times and any issues are dealt with promptly ■ Demonstrate the stated values of the organisation in all aspects of their representation of the team/Bureau ■ Ensure performance objectives, reviews and discussions are completed in line with Bureau policies and procedures for all direct reports ■ Conduct regular team meetings to share information and update staff on new requirements and policies ■ Support individual team members to achieve objectives, identify personal development opportunities, recognise areas of improvement and establish solution based outcomes ■ Participate in recruitment to attract the best person for the position and then ensure a complete and comprehensive induction takes place	■ Each team member understands clearly what is required of them and receives regular constructive feedback on progress ■ Each team member understands their contribution to IACD and Bureau outputs ■ Performance reviews are completed thoroughly and forwarded to the Unit Manager, Outreach & Engagement, within the specified timeframes ■ Employees have a training and development plan that is carried out in conjunction with L&D ■ Employees understand and demonstrate Bureau values in their day to day work ■ Employee issues (including non-performance issues) are successfully addressed in a timely manner ■ Leave liability is kept at a reasonable level ■ Staff are fully informed on relevant information, and organisation policies and procedures. ■ Team member skills are progressed as a result of mentoring and training ■ New staff are comprehensively inducted so that they are productive and comfortable in their role within 3 months
Coordination of Cyber Security consultancy services and related Information Assurance (IA) ■ Coordinating advice to Government departments, agencies and providers of Critical National Infrastructure through	■ Government departments, agencies and critical infrastructure operators are provided with actionable and timely policy and advice ■ Ensuring that customers receive relevant and timely consultancy advice from O&E team members or other technical experts

promoting national policy and standards and the provision of expert IT security advice and assistance ■ Acting as a lead Customer Relationship Manager for a portfolio of accounts ■ Ensuring the team remains situationally aware and public and sector alerts are highlighted as required ■ Utilising threat briefs and advisories to raise security awareness to Government or CNI as required ■ Contributing to the establishment, maintenance, promulgation and take-up of national policy and standards	in IACD ■ GCSB is seen as a credible source if information with increasing subscription lists and positive security effects ■ GCSB is invited to provide threat briefs and awareness briefs to CNI groups and public events ■ National policy and standards are relevant. Jobholder works closely with others responsible for the development of the Protective Security Requirements Framework to ensure that cyber security advice to government agencies is joined-up, relevant and timely
Liaison with international and domestic partner agencies, IT security community and industry ■ Participation in appropriate external Information Security and/or cyber security groups ■ Maintain an awareness of partner policies and standards ■ Coordinating Security Information Exchange forums ■ Maintaining a general awareness of the information security posture of industry players ■ Monitor business and external drivers that are likely to impact GCSB business ■ Maintain and enhance awareness of technology trends likely to impact on GCSB business	■ GCSB maintains a useful presence in the community by contributing and collaborating on cyber security issues. Access to partner advice and assistance is maintained ■ Secure Information Exchanges provide an effective forum for relevant information exchanges, leading to collaboration to address emergent threats ■ Collaboration is effective in countering the threat of technical attacks from hostile actors ■ Strong networks are developed and maintained to advance organisational aims. GCSB has a clear understanding of the IT security concerns of industry and community, and knows where IT security risks lie ■ Successful identification of future technology, CNI or business environment changes that impact on GCSB business ■ Provision of expert opinion and proposal of solutions in response to identified GCSB business gaps or problems

Note:

The above performance standards are provided as a guide only. The precise performance measures for this position will need further discussion between the jobholder and manager as part of the performance development process.

Person specification

Qualifications

Essential:	Desirable
■ Tertiary level qualification (Bachelor level) or equivalent experience in Information Technology, Computer Science or equivalent, with an emphasis on information security.	■ Tertiary papers in computer science, information security or information assurance. ■ Professional computing/networking qualification, e.g. in computer networking, or systems administration. ■ Professional Information Security certification.

Knowledge/experience

Essential:	Desirable:
■ Expert knowledge and 5 or more years' experience in IT security and/or information security policy, particularly computer security, network security and computer network defence ■ Highly developed communication skills ■ Highly developed negotiation and relationship management skills ■ Experience leading a team of security professionals	■ Experience with network assessment, defence and attack tools and techniques ■ Experience with operating systems administration ■ Experience as a security consultant ■ A good knowledge of network protocols ■ Experience with information security standards and frameworks ■ Programme or project management experience

Specialist competencies

The following would typically be expected for the 100% fully effective level

- The ability to exercise sound judgment together with a proven background in highly complex operational problem solving
- A good understanding of security risk assessment methodology
- A base level of understanding of enterprise architecture and design.
- The ability to formulate, interpret and apply information security policy in the context of computer and network security.
- A good understanding of technical security from experience in network and systems administration.

Core competencies

All employees are measured against the following core competencies as part of performance development

- Security

- Teamwork and Leadership
- Results Focus
- Communication and Knowledge Sharing
- Professionalism
- Innovation
- Customer Focus

Personal attributes

- Enthusiasm, self-motivation and innovation.
- Proven leadership qualities in a technical environment, and the ability to deal effectively and sensitively with other people.
- Highly effective planning and organisational skills.
- Highly developed oral and written communication skills, including the ability to communicate and build relationships at all levels; and to maintain a courteous, diplomatic and personable approach to customers and community partners.
- The ability to participate in management fora as an effective member of the team, and contribute to the development of a high performance organisation.
- The ability to represent the GCSB with credit within national and international communities.

Change 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. Such change may be initiated as necessary by the manager of this position. This position description may be reviewed as part of planning for the annual performance cycle.

Health & Safety

GCSB is committed to providing a healthy and safe work environment and safe management practices for all employees. Employees are expected to share this commitment as outlined in current Health and Safety legislation by taking all practicable steps to ensure:-

a. The employee's safety while at work, and

b. That no action or inaction of the employee while at work causes harm to any other person.

Knowledge Management

Employees are responsible for ensuring that all business records created are accessible and stored in the correct manner according to GCSB record keeping policy, standards and procedures

Employee: _____ Date: _____

Manager: _____ Date: _____