POSITION DESCRIPTION

Senior Policy Advisor, Information Security Policy and Research Unit

Unit/Branch, Directorate:	Information Security Policy and Research Unit, Information Assurance and Cyber Security Directorate
Location:	Wellington
Direct reports:	None
Salary range:	H $77,711 - $116,567

Purpose of position: The Senior Policy Advisor, Information Security Policy and Research (ISPR) Unit, is responsible for developing information security (INFOSEC) policy advice, analysis, and research on a range of issues for a variety of audiences. This role will support and contribute to directorate-wide policy and research projects, participate in interagency projects, and liaise with internal and external stakeholders on policy issues of significance.

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.

Key accountabilities	Deliverables/Outcomes
• Undertaking the research, analysis, consultation and development of national standards and information security policy	• Development of the Information security standards, policy, and guidance required by the NZ Government stakeholders • Policy and procedure analysis and creation is appropriately driven, conducted to a high standard, aligned to international best practice, and considers legal, regulatory, and policy issues as well as the business impact • Analysis undertaken is of a high quality and is recognised as significantly contributing to the NZ Government understanding of information security management • The use of conceptual frameworks that assist in the analysis and assessment of options and are able to convey abstract/complex ideas in practical terms appropriate for the audience • Able to identify risks and develop policy and process mitigations to manage the risk
• Promulgation of standards and guidance, ensuring our product is fit-for-purpose and accessible by stakeholders	• Customers and stakeholders are aware of changes to standards and guidance • All information security policy is maintained within an overarching, well organised, and cohesive portfolio • Standards and guidance are made accessible to customers via online platforms and other means in an accurate and timely manner
• Internal and external stakeholder and customer relationships are developed and maintained as required	• Internal and external stakeholders are engaged in a proactive, collaborative, and productive manner • The reputation of GCSB is positively viewed by other government agencies and key liaison stakeholders
• Under the direction of the Manager, areas requiring collaborative work with partner agencies including GCDO, GCDS GCPO, NCPO, PSR, and others are identified and prioritised as required	• Regular meetings are scheduled with all of the priority partner agencies (GCDO, GCDS, PSR, GCPO, DPMC) and others as required • Joint priorities and work programmes are supported with priority partner agencies
• Provide specialist policy advice concerning risk and compliance issues as they arise	• Quality and timely specialist advice is provided that supports the management of risk and compliance issues • The Unit's bespoke advice is actively sought by customers and stakeholders

• Develop policy responses at appropriate levels to meet strategic challenges (practitioner and strategic)	• Strategic decision makers and practitioners are informed of risks and provided with guidance where possible. Consideration is given to possible regulatory or legislative reform and requirements are developed to support this if necessary • The Unit is able to provide bespoke advice on risk and compliance issues when they arise • Customers are supported in the implementation of the standards, policy, guidance, advice where required
Health and safety (for self) • Work safely and take responsibility for keeping self and colleagues free from harm • Report all incidents and hazards promptly • Know what to do in the event of an emergency • Cooperate in implementing return to work plans • **Follow** GCSB's safety rules and procedures	• A safe and healthy workplace for all people using our sites as a place of work • 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:	None

Key stakeholders	
Internal:	• Information Assurance Units • IACD Communications team • NCSC units • GCSB legal and Compliance Teams • Any other IACD personnel as required • NZIC Joint Directors Office (JDO) • GCSB Intelligence Directorate (ID) • Other GCSB key stakeholders

External:	• The Government Chief Digital Officer (GCDO), DIA • The Government Chief Data Steward (GCDS), Statistics NZ • The National Cyber Policy Office (NCPO), within DPMC • Protective Security Requirements team (NZSIS) • NZSIS Security Services Group; • The Government Chief Privacy Officer (GCPO), DIA • CERT NZ, MBIE • Other NZ Government agencies where required • The academic and industry communities domestically and internationally • International policy counterparts. • IACD's customers

Person Specification	
Experience:	• Experience and a proven track record in public policy analysis • Experience on varied programmes of work, strategic and tactical skill, and able to ensure deadlines are met and product is fit-for-purpose
Knowledge and Skills:	**Essential**: • Ability to ensure the needs and demands of customers are balanced against an outcome sought by Government • Knowledge of applicable laws, regulation, information security policy, assurance frameworks, and the Governance mechanisms they sit within • Strong understanding of risk management practices at both the enterprise and all-of-government level • Ability to represent complex subjects with external stakeholders and forming consensus • Demonstrated ability to develop independent judgment across a range of complex areas • Self-motivated, innovative and possessing enthusiasm and drive • Strong interpersonal skills with the ability to foster good stakeholder relationships through consultation and partnership • Team player willing to support unit priorities when required

	• Highly developed oral and written communication skills, including the ability to present complex issues clearly, tailoring communications to meet audience needs • The ability to link strands of information together and evaluate the different aspects and impacts of issues • Demonstrated high levels of integrity • Demonstrated ability to work under pressure, meet deadlines, effectively allocate time within resource constraints and prioritise conflicting work demands **Desirable:** • Working knowledge of information security and broader security issues • Experience with the New Zealand Information Security Manual and Protective Security Requirements • Experience building strong relationships with external stakeholders across public, private and academia • A good understanding of contemporary legal trends and issues affecting the security sector • Understanding of New Zealand privacy law, regulation, and policy • Awareness of international trends in privacy, security, regulation and policy
Qualifications and Courses:	• A relevant tertiary qualification, preferably at post-graduate level, or equivalent experience • Information security industry qualifications and/or other specialist Information Assurance (IA) qualifications, is desirable
Specific Job Requirements:	• Ability to obtain and maintain a TSS security clearance

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: 24/08/2018

Signatures		
Manager's Name		
Signature		Date:

Employee's Name		
Signature		Date: