



POSITION DESCRIPTION

Digital Engagement Manager

Unit/Branch, Directorate: Outreach & Engagement, Information Assurance and Cyber Security Directorate

Location: Wellington or Auckland

Salary range: H \$77,711 - \$116,567

Purpose of position: Manage relationships with New Zealand Government agencies and critical national infrastructure owners in order to deliver cyber security services, liaison and outreach assistance through a range of outputs published via our digital platforms. A key component of this role will be the organisation and content management of our digital platforms.

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.

UNCLASSIFIED

Key accountabilities	Deliverables/Outcomes
<p>Cyber Security consultancy services and related Information Assurance (IA)</p> <ul style="list-style-type: none"> • Establishes, builds and maintains highly effective working relationships with internal and external stakeholders • Acts as the key communication conduit between external agencies and GCSB, ensuring information flows appropriately and all parties are actively engaged • Works collaboratively with managers and key staff across GCSB to produce advice and guidance to Government departments, agencies and significant national organisations • Promotes national policy and creates digital artefacts for the provision of expert IT security advice and assistance avoiding duplication of effort and expense • Maintains situation awareness of cyber security issues and threats and ensures that advice and guidance delivered via our digital platforms is up to date, accurate and timely • Takes action to produce suitable artefacts to educate the security communities of interest to raise security awareness of cyber security and IA issues in Government or significant national organisations as required • Advocates for the establishment, maintenance, promulgation and take-up of national policy and standards 	<ul style="list-style-type: none"> • Government departments, agencies and significant national organisations' operators are provided with actionable and timely written policy and advice • GCSB is seen as a credible source of information and positive security advice and Government departments, agencies and significant national organisations' operators actively seek advice and support • GCSB is invited to provide cyber security education • Job holder has established close working relationships with others responsible for the development of the Protective Security Requirements Framework and ensures that cyber security advice to government agencies is joined-up, relevant and timely
<p>Liaison with international and domestic partner agencies, IT security community and industry</p> <ul style="list-style-type: none"> • Maintain an awareness of partner policies and standards • Develop guidance and advice artefacts to support education events and forums such as the Security Information Exchange Forums • Collect, collate information on cyber security events, incidents and produce useful information to support raising the cyber resilience of customers • Monitor and manage all digital platforms to ensure customer access is maintained at all times 	<ul style="list-style-type: none"> • Secure Information Exchanges provide an effective forum for relevant information exchanges, leading to collaboration to address emergent threats • Strong networks are developed and maintained to advance organisational aims. GCSB/NCSC 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, significant national organisations or business environment

UNCLASSIFIED

<ul style="list-style-type: none"> • Manage personal tasking, and remain aware of Unit-wide operational developments, to ensure timeliness and deliverables • Maintaining a general awareness of the IT security posture of the industry players • Monitor business and external drivers that are likely to impact GCSB/NCSC business • Maintain and enhance awareness of technology trends likely to impact on GCSB/ NCSC business 	<p>changes that impact on GCSB/NCSC business</p> <ul style="list-style-type: none"> • Provision of expert opinion and proposal of solutions in response to identified GCSB/NCSC business gaps or problems
<p>Delivery of output</p> <ul style="list-style-type: none"> • Produce timely and relevant cyber security related reporting for customers, based on material obtained from classified and unclassified sources • Enhance GCSB’s relationships and reputation with customers and partners through professional representation and engagement. Ensure output capabilities and limitations are known to customers where appropriate • Communicate effectively with teams within GCSB, and within external customer and partner agencies 	<ul style="list-style-type: none"> • O&E Unit provides timely and accurate technical advice and expertise digitally • Campaign artefacts meet all required quality standards, as specified in relevant policy documentation • Artefacts are created to reflect guidance in the New Zealand Information Security Manual (NZISM) and Protective Security Requirements (PSR) advice, and do not violate compliance rules, and any inadvertent breaches are notified to Compliance and dealt with appropriately • Productive and enduring relationships are formed with domestic and international partners • O&E Unit has a detailed awareness of customers’ needs and expectations • Customer enquiries are attended to in a timely manner
<p>Contribute to the execution of the IACD Plan</p> <ul style="list-style-type: none"> • Promoting cross-team collaboration through the execution of the IACD Plan and support for 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 	<ul style="list-style-type: none"> • Contributing through participation in cross-functional IACD teams to the development, refinement and execution of the plan • Customer feedback suggests that the plan is having a positive effect on IACD’s performance through the creation of an improved operating model • Confident about and responsible for proposing amendments to the plan and ensuring that they are enacted

UNCLASSIFIED

<p>Health and safety (for self)</p> <ul style="list-style-type: none"> • 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 • Be a visible role model at all times • Follow GCSB's safety rules and procedures 	<ul style="list-style-type: none"> • 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
<p>Other duties</p>	<ul style="list-style-type: none"> • Administering the loading of content and customer accounts on the Portal, and content for the website • Contributing to future digital platform development strategy and implementation of roadmap

Position delegation	
Financial delegation:	None

Key stakeholders	
Internal:	<ul style="list-style-type: none"> • New Zealand Intelligence Community • NZ Government departments and agencies • NZ significant national organisations • As necessary, other private or commercial organisations with cyber security interests
External:	<ul style="list-style-type: none"> • Outreach and Engagement Management staff • 3rd party design/marketing organisations • GCSB staff

Person Specification	
Experience:	<ul style="list-style-type: none"> • At least 3 years marketing and/or journalistic experience • Expert writing skills and the ability to translate technical information in to easily consumable products • An interest or experience in writing content on Information technology or Information security topics

UNCLASSIFIED

Knowledge and Skills:	<ul style="list-style-type: none">• Sound working knowledge of frameworks, processes and methodologies that contribute to excellent marketing material• Highly developed communication skills• Strong relationship management skills• Digital user interface experience, is desirable• Experience using web based tools for customer engagement, is essential• Programme or project management experience, is desirable
Qualifications and Courses:	<ul style="list-style-type: none">• Tertiary level qualification (Bachelor level) or equivalent• Tertiary papers in journalism or marketing
Specific Job Requirements:	<ul style="list-style-type: none">• Ability to obtain and maintain a TSS security clearance• Must have an interest in IT and preferably Information Security topics

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.

The position is aligned to the Service Delivery and Engagement competency framework.

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.

UNCLASSIFIED

Date PD reviewed: 2/08/2018

Signatures		
Manager's Name		
Signature		Date:

Employee's Name		
Signature		Date:



GOVERNMENT
COMMUNICATIONS
SECURITY BUREAU
TE TIRA TIAKI

**BEYOND
ORDINARY**
We are. Are you?