Australian Government

ANSTO
Science. Ingenuity. Sustainability.

POSITION DESCRIPTION

Position Title:	Cyber Security ~~Officer~~Administrator
Cluster / Business Unit / Division	Enabling
Section or Unit:	Information Technology
Classification:	Band 5/6
Position Description Number:	PD-2056
Work Contract Type:	Professional

POSITION PURPOSE

The Cyber Security Officer is instrumental in the development, maintenance and support of ANSTO's Cyber and Digital Security function. This role contributes to the development of ANSTO's digital capacity and capability through innovation in cyber security initiatives; responding to cyber security incidents; identifies and analyses cyber and digital security requirements and provides expert advice on the application of best practice cyber security across all computer based systems and services at ANSTO.

ORGANISATIONAL ENVIRONMENT

ANSTO leverages great science to deliver big outcomes. We partner with scientists and engineers and apply new technologies to provide real-world benefits. Our work improves human health, saves lives, builds our industries and protects the environment. ANSTO is the home of Australia's most significant landmark and national infrastructure for research. Thousands of scientists from industry and academia benefit from gaining access to state-of-the-art instruments every year.

This role is within the Information Technology division who are responsible for the delivery of IT services across ANSTO. IT are responsible for day to day IT service delivery and support and also the execution of large capital projects.

Information Technology is dedicated to enhancing and maintaining ANSTO's digital facilities for operational reliability and, providing a range of customer services to support ANSTO's research, business activities and projects.

Cyber Security is comprised of a range of disciplines structured to support and protect ANSTO's IT and OT assets, personnel and information and to provide safeguards against internal and external threats.

ACCOUNTABILITIES & RESPONSIBILITIES

Key Accountabilities

Band 5 level:

- Identify and analyse cyber security requirements and develop appropriate measures to ensure confidentiality, integrity and availability of ANSTO's IT and OT environments in accordance with industry practice and government policy
- Implement, monitor and maintain cyber security systems and respond to cyber security incidents using appropriate tools, techniques and procedures, to maintain ANSTO's safe, secure and sustainable operations
- Provide expert risk based advice, educate and inform stakeholders at all levels on their obligations relating to cyber security and compliance to ensure the application of a contemporary digital environment across ANSTO on a consistent basis

- Ensure compliance with national security regulations, standards, architectures and policies necessary to ensure effective security outcomes across all aspects of the organisation
- Support the broader operation of digital services by working co-operatively with other teams within and beyond IT to ensure agreed information security processes are adhered to within defined service levels, proactively share knowledge and participate readily in continual service improvement
- Contribute to the branch/division business and strategic planning and capacity building; advocate new approaches to achieving organisational outcomes based on sound evidence and professional knowledge; provide technical guidance for the agency security program
- Develop and manage effective relationships and partnerships with key internal and external stakeholders; facilitate ongoing consultation, the exchange of information and foster optimal contribution and engagement; facilitate communications between security personnel, IT personnel and business personnel to ensure alignment of business and security objectives
- Liaise with external intelligence agencies, monitor threat feeds and communicate applicable threat information
- Conduct security risk assessments, audits and reviews
- Undertake additional duties as required and during periods of leave of other staff

Band 6 level:

- Minimum 1 year or equivalent experience performing Band 5 accountabilities.
- Undertakes the above key accountabilities independently with little or no direct supervision.
- Independently exercises sound individual judgement and applies cyber security knowledge and experience to troubleshoot, investigate and resolve complex incidents and other issues.
- Proven ability to manage projects and/or significant incidents from concept to completion.
- Utilises sound judgement to independently assess priorities of projects and incidents to optimise the allocation of resources.
- Demonstrated ability to lead and coordinate small teams to achieve outcomes with little or no supervision.
- Demonstrated ability to proactively contribute to the process of continual improvement in safety, security and performance and the knowledge and competency of individuals in the team.
- Demonstrated ability to coach, mentor and co-ordinate other staff.

Decision Making

- The position works within a framework of legislation, policies, professional standards and resource parameters. Within this framework the position has some independence in determining how to achieve objectives, including deciding on methods and approaches, unit operations, project planning and allocation of resources.
- The position is fully accountable for the accuracy, integrity and quality of the content of advice provided internally and is required to ensure that decisions are based on sound evidence, but at times may be required to make effective judgements under pressure or in the absence of complete information or expert advice.
- The Cyber Security Officer determines key work priorities within the context of agreed work plans and will consult with management on complex, sensitive and major issues that have a significant impact on the organisation.

- The levels of authority delegated to this position are those approved and issued by the Chief Executive Officer. All delegations will be in line with the ANSTO Delegation Manual AS-1682 (as amended or replaced).

Key Challenges

- Achieving improved governance such that standards are continually strengthened, developed and applied in a consistent manner and reflect best practice
- Improving the responsiveness of the organisation to deliver on operational and strategic cyber security related requirements
- Contributing to enhancing a strategically led culture focussed on ensuring change is managed appropriately and effectively and is aligned to ANSTO's strategic objectives.
- Engaging and influencing stakeholders to ensure relevant cyber and digital security measures and risk management frameworks are developed and implemented.
- Maintaining currency with contemporary developments in regulatory and legislative requirements and organisational policies relating to cyber security and risk management.
- Coordinate communication between security and business functions, as well as manage and understand the application of controls and security risk management processes

KEY RELATIONSHIPS

Who	Purpose
Internal	
Chief Information and Digital Officer	• Receive guidance and direction • Provide expert, authoritative and evidence based advice on cyber and digital security • Recommend and gain endorsement for improvement or development plans and goals and other initiatives
Cyber Security and OT Manager	• Provide expert, authoritative and evidence based advice on cyber and digital security • Provide timely advice and reporting on cyber and digital security related requests • Assist in organisational activities ensuring protection of ANSTO information assets • Report residual risks, outstanding threats, findings or incidents that may impact ANSTO
Work area team members	• Provide expert advice and analysis on a full range of matters • Contribute to executive decision making processes, strategic planning and goals • Collaborate and share accountability • Negotiate and resolve conflicts
ANSTO Clusters	• Engage, consult regularly to identify cyber and digital security requirements • Provide expert advice and exchange information • Collaborate on cross cluster/organisation projects
External	
Stakeholders	• Develop and manage effective partnerships to collaborate on Cyber Security, Risk and Assurance activities • Participate in International Atomic Energy Agency (IAEA) activities such as; delivering international cyber security training courses,

	developing and reviewing nuclear cyber security standards

POSITION DIMENSIONS

Staff Data	
Reporting Line	Reports to the Cyber Security and OT Manager
Direct Reports	None
Indirect Reports	TBA

Financial Data (2015/2016)
Revenue / Grants
Operating Budget
Staffing Budget
Capital Budget
Assets

Special / Physical Requirements	
Location:	Lucas Heights Working in different areas of designated site/campus as needed
Travel:	May be required to travel to ANSTO sites and other organisations from time to time involving occasional national travel Infrequent international travel
Physical:	Office based physical requirements (sitting, standing, minimal manual handling, movement around office and site, extended hours working at computer)
Radiation areas:	May be required to work in radiation areas under tightly regulated conditions
Hours:	Willingness to work extended and varied hours based on operational requirements
Clearance requirements:	Satisfy ANSTO Security and Medical clearance requirements Successful candidate will be required to obtain Negative Vetting 1 Security Clearance

Workplace Health & Safety	
Specific role/s as specified in AG-2362 of the ANSTO WHS Management System	All Workers Other specialised roles identified within the guideline a position holder may be allocated to in the course of their duties

ORGANISATIONAL CHART

TBA

KNOWLEDGE, SKILLS AND EXPERIENCE

Band 5

1. Tertiary qualifications in an appropriate discipline, and/or demonstrable extensive experience in the delivery of a significant portfolio of IT services.
2. Capacity to contribute to the management of change with the view of continuously improving the organization.
3. Experience and understanding of technical, policy and human dimensions of Cyber Security in a complex environment responsible for running a variety of services.
4. Demonstrated capacity in identifying, assessing and managing risks in the enterprise along with the ability to provide a high level of assurance to internal/ external stake holders.
5. High level interpersonal, communication (oral, written, listening and presentation), teamwork and customer service skills.

Band 6

1. Experience in leading and managing change in a continually evolving environment.
2. Demonstrated experience managing operating, project and capital budgets.
3. Extensive experience in the development and implementation of cyber security policies and standards.

The transition from Band 5 to Band 6 will occur following a recommendation from the relevant manager, assessment by management and approval from the CIDO. Transition is not automatic and ability to perform Band Y accountabilities will need to be demonstrated and assessed.

VERIFICATION

This section verifies that the line manager and appropriate senior manager/executive confirm that this is a true and accurate reflection of the position.

Line Manager		**Delegated Authority**	
Name:	Nick Howarth	Name:	Marianne Morton
Title:	Cyber Security and Operational Technology Manager	Title:	Chief Information Digital Officer
Signature:		Signature:	
Date:		Date:	

Cyber Security Officer Linked Role (PD-2056) Band 5 to Band 6 Transition Checklist	
Name:	
Commencement Date:	
Assessment Date:	

Note: Full written submission demonstrating and justifying how the employee meets the requirements must also be attached.

Requirements for transition	Met Criteria
Demonstrated examples of knowledge, skills and experience expectations at a Band 6 level of competence	☐ Yes ☐ No
Demonstrable extensive experience in the delivery of a significant portfolio of IT services.	☐ Yes ☐ No
Contributions to the management of change with the view of continuously improving the organization.	☐ Yes ☐ No
Experience and understanding of technical, policy and human dimensions of Cyber Security in a complex environment responsible for running a variety of services.	☐ Yes ☐ No
Demonstrated capacity in identifying, assessing and managing risks in the enterprise along with the ability to provide a high level of assurance to internal/ external stake holders.	☐ Yes ☐ No
High level interpersonal, communication (oral, written, listening and presentation), teamwork and customer service skills.	☐ Yes ☐ No
Demonstrated experience managing operating, project and/or capital budgets.	☐ Yes ☐ No
Extensive experience in the development and implementation of policies and standards.	☐ Yes ☐ No
Experience in leading and managing change in a continually evolving environment.	☐ Yes ☐ No