Australian Government

ANSTO
Science. Ingenuity. Sustainability.

POSITION DESCRIPTION

Position Title:	Cyber Security Manager
Cluster / Business Unit / Division	Information Technology
Section or Unit:	Cyber Security and Operational Technology
Classification:	Band 7
Job Family:	Information Technology
Position Description Number:	PD-2405
Work Contract Type:	Management
STEMM/NON-STEMM:	STEMM
STEMM Category:	Technology

POSITION PURPOSE

The Cyber Security Manager is responsible for developing and implementing ANSTO's strategic Cyber Security Risk, Governance, Assurance, Incident Response and Asset Management standards, while providing leadership, guidance and support to the ANSTO Cyber Security Team, IT and OT Asset Managers across the organisation. The Cyber Security Manager ensures compliance with cyber security and asset management policy, standards, regulations and legislation across all of ANSTO's IT and OT assets.

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.

The Information Technology division enhances and maintains ANSTO's digital facilities for operational reliability and provides a range of customer services to support ANSTO's research, business activities and projects.

Within the Cyber Security and Operational Technology group, the Cyber Security team develops and implements ANSTO's cyber security risk management plan across the organisation following international and national nuclear cyber security guidance covering risk, governance, protection, detection and response to cyber security threats and vulnerabilities.

The Cyber Security Manger works closely with the General Manger, Cyber Security and Operational Technology and may be required to provide backup to them on occasion.

ACCOUNTABILITIES & RESPONSIBILITIES

Key Accountabilities

- Evolve, implement and monitor a strategic, comprehensive cyber security risk management framework and asset management program across all of ANSTO's technology landscape in line with statutory, regulatory and policy requirements, supporting the safe, secure and sustainable value generation of these assets.
- Drive the implementation of the cyber security risk management framework within current and future projects and other initiatives both within IT and across other business units.
- Plan and execute an ongoing programme of cyber security control verification and related assurance activities across ANSTO's entire technology landscape of IT and OT systems.
- Lead cyber security incident response activities involving the cyber team, and relevant subject matter experts and stakeholders.

- Oversee risk and audit programs in line with organisational processes across portfolios within ANSTO's IT and OT environment ensuring transparency, accountability and risk minimisation ensuring compliance with industry best practice standards and relevant statutory requirements
- Develop and manage effective partnerships and reporting with key internal and external stakeholders.
- Contribute to strategic planning, providing a current knowledge and future vision of cyber security risk management approaches, cyber security control technologies, practices and processes.
- Advocate and influence the ingestion, analysis, dissemination and application of cyber security threat intelligence.
- Influence the desired cyber security culture across ANSTO to ensure safe, secure and sustainable workplace culture and behaviours.
- Undertake additional duties as required and during periods of leave of 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 position determines key work priorities within the context of agreed work plans and will consult with the General Manager, Cyber Security and Operational Technology 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

- Maintaining currency with contemporary developments in threat, risk, regulatory and legislative requirements and organisational policies relating to cyber security and enterprise risk management.
- Leading, influencing, and managing a high performing team of multidisciplinary cyber security professionals.
- 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 security controls are developed, implemented and sustainably maintained.
- Developing innovative and creative solutions to complex new or undefined cyber security risks and issues.
- Maintaining an accurate and current view of all cyber security services and their asset management and risk profiles.
- Developing and maintaining knowledge of ANSTO's IT and OT systems given the complexity, diversity and uniqueness of the systems which in many cases are unique in the world.
- Interacting with customers to manage their expectations given constraints that may be imposed by financial, technical, resource, safety or regulatory requirements.
- Dealing with ambiguity and a rapidly changing environment.

KEY RELATIONSHIPS

Who	Purpose
Internal	
Chief Information and Digital Officer	• Receive guidance and direction. • Provide expert and strategic advice and plans in relation to the strategy, implementation, development and maintenance of ANSTO's cyber security risk management framework. • Provide expert advice and recommendations with respect to emergent or ongoing cyber security incident response activities.
General Manager, Cyber Security and Operational Technology	• Receive guidance and direction. • Provide expert and strategic advice and plans in relation to the strategy, implementation, development and maintenance of ANSTO's cyber security risk management framework. • Recommend and gain endorsement for improvement or development plans and goals and other initiatives.
Cyber Security Team	• Provide leadership, direction and support. • Set performance requirements and manage performance and facilitate ongoing professional development. • Engage to monitor trends, performance and progress against strategic plans and evaluate further support which may be required to ensure delivery against the plans.
ANSTO IT and OT Asset Owners and Divisional Stakeholders	• Engage, consult regularly and collaborate on project development and delivery. • Establish, and manage agreed cyber security improvements to systems that meet risk, research, business and regulatory needs. • Provide expert advice and exchange information. • Collaborate on cross cluster/organisation projects.
External	
Stakeholders/Vendors	• Develop and manage effective relationships to collaborate on cyber security initiatives, projects, and delivery including domestic and international nuclear, government, industrial, and academic collaborators e.g. Australian Cyber Security Centre, International Atomic Energy Agency • Effectively exchange information with external stakeholders and vendors

POSITION DIMENSIONS

Staff Data	
Reporting Line	Reports to the General Manager, Cyber Security and Operational Technology.
Direct Reports	3
Indirect Reports	OT Leads and Project resources

Financial Data	
Revenue / Grants	n/a
Operating Budget	$1.6M
Staffing Budget	$0.5M
Capital Budget	$0.0M
Assets	$2.5M

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 and international travel
Physical:	Office based physical requirements (sitting, standing, minimal manual handling, movement around office and site, extended hours working at computer) Presentations/Public speaking
Radiation areas:	Not required to work in radiation areas
Hours:	Ability to work extended and varied hours based on operational requirements May be required to provide out-of-hours support during incident response
Clearance requirements:	Satisfy ANSTO Security and Medical clearance requirements Negative Vetting 1 Security Clearance

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

ORGANISATIONAL CHART

On File

KNOWLEDGE, SKILLS AND EXPERIENCE

1. Degree in Information Technology, Cyber Security or other relevant discipline and/or extensive experience with cyber security engineering across a range of facilities and technologies.
2. Knowledge and experience of relevant cyber security standards and guides including a detailed understanding of IEC 62443, NIST SP 800-82, ISO/IEC 27001, ASD ISM, IAEA NSS 17-T.
3. Understanding and experience in the application of ISO55000 asset management principles and practices.
4. Understanding and experience in ITIL or equivalent IT Service Management (ITSM) principles and practices.
5. IT or engineering project management experience.
6. Experience working under a strict quality assurance system in a tightly regulated environment.
7. Understanding of safety management standards and practices.
8. Problem solving skills and the ability to assess and resolve complex technical issues.
9. Demonstrated organisational skills including the ability to apply judgement to manage demanding workloads and conflicting priorities, prioritise tasks and meet deadlines.
10. Excellent interpersonal and communication skills, both verbal and written across all organisational levels.
11. Proven ability to show initiative in working independently, be deadline driven, and reliable in following through with actions.
12. Budget management experience, including cost analysis and business case development.
13. Demonstrated understanding of and responsiveness to the needs of customers, service providers and stakeholders.

14. Experience in executive technology decisions making, including managing diverse teams of direct and indirect reports and other management and executive stakeholders in a results-focused environment, including experience mentoring/coaching and negotiating.

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:	General Manager, Cyber Security and Operational Technology	Title:	Chief Information and Digital Officer
Signature:		Signature:	
Date:		Date:	