Australian Government

ANSTO
Science. Ingenuity. Sustainability.

POSITION DESCRIPTION

Position Title:	Operational Technology Manager
Cluster / Business Unit / Division	Information Technology
Section or Unit:	Cyber Security and Operational Technology
Classification:	Band 7
Job Family:	ICT & Digital Solutions
Position Description Number:	PD-2204
Work Contract Type:	Professional
STEMM/NON-STEMM:	STEMM

POSITION PURPOSE

The Operational Technology (OT) Manager is responsible for developing and implementing ANSTO's strategic OT architecture and technology standards, while providing leadership, guidance and support for ANSTO's OT and related engineers and technicians. The OT Manager ensures compliance with asset management and cyber security policy, standards, regulations and legislation across all of ANSTO's OT assets. The role's focus is on standardisation, risk management, assurance and mitigation; contributing to the development of ANSTO's OT asset management and cyber security capacity and capability.

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 Operational Technology team designs, implements, and maintains a wide range of ANSTO's Operational Technology assets together with providing strategic governance, guidance and engineering support to other operational technology asset owners and managers across the organisation.

ACCOUNTABILITIES & RESPONSIBILITIES

Key Accountabilities

- Develop, implement and monitor a strategic, comprehensive operational technology strategy and asset management program across ANSTO in line with statutory, regulatory and policy requirements, supporting the safe, secure and sustainable value generation of these assets.
- Drive the implementation of the ANSTO-wide OT architectural and technology standards within current and future facilities.
- Auditing existing campus and facility OT, IoT, robotics and related infrastructure and developing a program of works to mitigate and manage asset management and cyber security risks on a continuing basis.
- Develop and manage effective partnerships and reporting with key internal and external stakeholders; facilitate ongoing consultation, the exchange of information and fostering optimal contribution and engagement; facilitate communications between Operational Technology stakeholders, IT, security, engineering, research and other business units to ensure alignment of asset management, business and security objectives for ANSTO OT.

- Lead and Chair the ANSTO Operational Technology Community of Practice, ensuring ongoing governance, communication and collaboration across the OT technical teams.
- Understand and interact with related and external disciplines to ensure the consistent application of policies and standards across all OT projects, systems and services.
- Assist with the overall IT and OT strategic planning, providing a current knowledge and future vision of technology and systems.
- Manage resources to ensure compliance with relevant organisational policies, practices and, where appropriate, statutory requirements. Prepare budgets for operating and project responsibilities within portfolio environment.
- Oversee risk, audit and assessment programs in line with organisational processes across portfolios within ANSTO's OT environments ensuring transparency, accountability and risk minimisation ensuring compliance with industry best practice standards and relevant statutory requirements.
- Lead and manage a multi-disciplinary team with a focus on effective development and deployment of capabilities to maximise customer satisfaction and operational outputs; facilitate ongoing professional development using appropriate coaching and mentoring techniques, training, participation in development opportunities aligned to their role and development plan in accordance with policy.
- Be the single point-of-contact in the IT division for early and ongoing engagement on all technical engineering projects related to OT, including projects managed by individual facilities.
- Reinforce the desired culture within the OT engineering and technical teams to ensure safe, secure and sustainable workplace culture and behaviours.
- Allocate and monitor the progress of GRC investigations, incident response and actions assigned to staff within the OT technical teams & completion of assigned events and actions.
- Undertake additional duties as required and during periods of leave of other staff including General Manager Cyber Security and Operational Technology.

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 operational technology asset, cyber and risk management.
- Leading, influencing, and managing a high performing team of multidisciplinary operational technology professionals as indirect reports.
- 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 operational technology measures and risk management frameworks are developed, implemented and sustainable.
- Developing innovative and creative solutions to complex new or undefined OT engineering and cyber security risks and issues

- Maintaining an accurate and current view of all OT systems and their asset management and cyber security risk profiles.
- Developing and maintaining knowledge of ANSTO's 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.
- Working in a matrixed structure in a hierarchical organisation

KEY RELATIONSHIPS

Who	Purpose
Internal	
General Manager, Cyber Security and Operational Technology	• Receive guidance and direction. • Provide expert and strategic advice in relation to the strategy, implementation, development and maintenance of ANSTO's OT asset management and cyber security standards. • Recommend and gain endorsement for improvement or development plans and goals and other initiatives.
Work Area Team Members	• Provide expert advice, technical and otherwise on a full range of matters. • Contribute to management decision making processes, strategic planning and goals. • Collaborate and share accountability. • Negotiate and resolve conflicts.
Direct and Indirect Reports, OT Technical Teams	• 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 OT Asset Owners and Divisional Stakeholders	• Engage, consult regularly and collaborate on project development and delivery. • Establish, and manage agreed OT asset management and 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 OT and cyber security initiatives, projects, and delivery including domestic and international nuclear, government, industrial, and academic collaborators e.g. Engineers Australia, the 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	4

Indirect Reports	Approximately 10 OT/I&C Engineers, both operational and project delivery across the organisation.

Financial Data	
Revenue / Grants	n/a
Operating Budget	$0.6M
Staffing Budget	$0.2M
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:	May be required to work in radiation areas under tightly regulated conditions
Hours:	Ability to work extended and varied hours based on operational requirements May be required to provide out-of-hours support
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. University degree in Controls Engineering, Information Technology, Cyber Security or other relevant discipline or equivalent experience.
2. 5+ years OT and/or cyber security engineering experience across a range of facilities and technologies.
3. 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 NSS017 and NST047.
4. Cyber security industry accreditations (e.g.. CISSP, CEH, CISM, CISA, GIAC) are desirable.
5. Understanding and experience in the application of ISO55000 asset management principles and practices.
6. Knowledge of ANSTO OT facilities, systems and associated procedures and regulatory processes.
7. Engineering project management experience.
8. Experience working under a strict quality assurance system in a tightly regulated environment.
9. Understanding of safety management standards and practices.

10. Problem solving skills and the ability to assess and resolve complex technical issues.
11. Demonstrated organisational skills including the ability to apply judgement to manage demanding workloads and conflicting priorities, prioritise tasks and meet deadlines.
12. Excellent interpersonal and communication skills, both verbal and written across all organisational levels.
13. Proven ability to show initiative in working independently, be deadline driven, and reliable in following through with actions.
14. Demonstrated experience managing budgets.
15. Demonstrated understanding of and responsiveness to the needs of customers, service providers and stakeholders relevant to OT and cyber security.
16. Demonstrated leadership experience in a results-focused environment, including experience mentoring/coaching and negotiating with technicians, engineers and leaders.
17. Personal qualities that add value to a team operating in a high level client service / safety, security & quality environment.

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:	