Position Description

TasNetworks | Powering a Bright Future

Cyber Security Operational Technology Specialist

Digital, Strategy & Customer | Cyber Security

Objectives	• Responsible for designing, governing, and assuring secure OT and industrial control system (ICS) environments across the organisation. • Provide strategic and technical leadership for cyber security architecture across critical infrastructure, industrial automation, SCADA and converged IT/OT environments. • Ensure and embed "security by design" principles into all TasNetworks' activities to ensure our assets, data and reputation are protected from cyber security threats • Establish target-state security architectures, standards, reference patterns, and secure-by-design principles aligned to enterprise risk appetite, regulatory obligations, and operational resilience objectives
Role Specific Accountabilities	• Lead enterprise cyber security improvements and risk reduction through the end-to-end technology asset lifecycle, with awareness of the organisation's risk and threat profile. • Own and maintain the enterprise OT cyber security architecture, strategy, and roadmap, ensuring alignment with business objectives, operational resilience requirements, and critical infrastructure obligations. • Establish and govern target-state architectures, security standards, principles, reference architectures, and design patterns for OT and industrial environments. • Ensure security architecture aligns with business strategy, operational resilience, and regulatory obligations. • Provide high level strategic, as well as tactical and operational cyber security advice to Operational Technology teams, Strategic Asset design teams, Digital Technology teams, and Cyber Security Project teams. • Support the successful handover and transition to business as usual for new cyber security related standards, processes, procedures and technologies as they are delivered by the Cyber Security Program of Work. • Identify, assess, prioritise, and coordinate the protection of critical infrastructure and energy delivery automation systems. • Keep abreast of technological advancements, compliance requirements, and operational technology cyber security best practices for the electric power network. • Any other duty or tasks as reasonably and lawfully directed by TasNetworks.

To be successful in this role	• Degree qualification in Cyber Security, Information Technology, Engineering, or related discipline. • Significant experience in cyber security architecture within OT/ICS environments. • Demonstrated experience designing secure OT and industrial network solutions. With an understanding of – SCADA, PLCs, DCS environments, Industrial protocols, IT/OT convergence. • Experience implementing or governing security frameworks such as IEC 62443, NIST, ISO 27001, or PSPF. • Strong stakeholder engagement and influencing capability across technical and operational audiences. • Demonstrated ability to lead solution governance and provide strategic security direction. • Experience supporting critical infrastructure or high-availability operational environments. • Industry certifications such as – CISSP, SABSA, TOGAF, GIAC GICSP would be an advantage. • Knowledge of Australian critical infrastructure legislation and obligations. • Demonstrate our Core Capabilities, which are central to all positions at TasNetworks. • A strong understanding and awareness of cyber security concepts, concerns, controls, and frameworks, especially the AESCSF, but also NIST CSF, CIS Critical Security Controls, ACSC Essential 8, etc. • Commercial astuteness and a results-driven approach. • Proven ability to innovate and identify opportunities to improve efficiencies in project delivery processes. • Strong leadership and influencing skills, including the ability to build and leverage strong customer and stakeholder relationships. • Exceptional organisation, coordination and time management skills (action orientated). • A strategic mind-set, the ability to think 'outside the box', and a propensity to truly challenge the status quo. • Relevant utility / industry experience, skills, and knowledge are highly desirable. • Able to demonstrate the capacity to perform the inherent requirements of the role.

Compliance Requirements	• A satisfactory National Police Record check to confirm eligibility for the role
	
	• A 'critical worker' suitability assessment for the purposes of the *Security of Critical Infrastructure Act 2018* (Cth) (or any successor to that Act) and the *Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules 2023* (Cth) (or any successor to those Rules), comprised of:
	  ○ a National Security Assessment by ASIO;
	  ○ a Criminal History Check by ACIC; and
	  ○ a Right to Work in Australia check;

Reports to:	Direct reports:	Approved:
Leader Cyber Operations	0	June 2026