ARPC Position Description

Role title:	Head of Information Security		
Function:	Information Security	**Classification broadband:**	EL2
Location:	Sydney	**Security clearance:**	NV1
Role reports to (role title):	Chief Operating Officer (COO)		
Direct reports (role titles):	2 direct reports - Manager Cyber Security, Information Security Analyst External Partners (CyberCX, AXE) as required		

Purpose of the role (Why the role exists; how the role contributes to the ARPC's strategic objectives)

Reporting to the Chief Operating Officer (COO), the Head of Information Security leads ARPC's enterprise approach to cyber security covering strategy, implementation, compliance, and incident response.

A core accountability of the role is to advise, write for, and present to the ARPC Board and its Committees supporting the COO, ensuring the Board has clear, timely, and risk-informed visibility of ARPC's cyber security posture.

The position provides strategic direction and practical leadership to protect ARPC's information assets and maintain compliance with Government and organisational standards. The role also carries responsibility as ARPC's Information Security Adviser under the Protective Security Policy Framework (PSPF) for Government.

Key accountabilities (Key activities, tasks and outcomes to be achieved)

Board Reporting and Advisory

- Prepare, write, and present high-quality cyber security papers and reports to the ARPC Board and Risk Committee supporting the COO, providing clear, risk-informed insights into ARPC's cyber posture, key risks, and investment priorities.
- Advise the Board and Committees supporting the COO on emerging threats, compliance obligations, and strategic priorities to support effective oversight and decision-making.
- Ensure Board reporting is integrated with executive risk management processes and aligned to ARPC's enterprise governance frameworks

Leadership and Management

- **Team Leadership**: Provide clear direction, coaching, and support to internal team members, fostering a high-performance culture and continuous capability uplift in cybersecurity awareness and technical proficiency.
- **Partner Management**: Oversee relationships with external cybersecurity partners, including managed service providers, ensuring service delivery meets agreed standards, contractual obligations, and ARPC's security requirements.
- Role model ARPC's Values and Code of Conduct and Capabilities set out in ARPC's Capability Framework

Strategic Oversight

- Lead and continuously evolve ARPC's Information Security Strategy, ensuring alignment between strategic intent and operational execution.
- Own ARPC's Information Security Policy and Strategy, providing direction and oversight for their effective implementation across the enterprise in partnership with the Technology Team.
- Ensure ongoing compliance with the PSPF, Information Security Manual (ISM), Essential Eight, Privacy Act, and other applicable legislative and policy frameworks.
- Oversee governance and management of emerging security risks including those related to artificial intelligence, cloud services, and third-party environments ensuring alignment with government and industry best practice standards

Cyber Risk & Assurance

- Prepare and present high-quality papers and reports to the Board and Risk Committee, delivering clear insights on ARPC's cyber posture, key risks, and investment priorities.

  - Maintain and continuously improve the Information and Cyber Security Risk and Control Library, ensuring accuracy, traceability, and alignment with ARPC's enterprise risk management framework.
  - Lead cyber risk management, assurance, logging and incident response activities to maintain cyber exposure within approved risk appetite.
  - Define, implement, and monitor data loss prevention and protection controls in close partnership with the Technology Team.
  - Establish, govern, and monitor Zero Trust Network Access (ZTNA) and Security Platform (e.g. EDR/XDR) policies, ensuring compliance, operational effectiveness, and continuous improvement
- **Organisational Awareness & Training**
  - Lead the design and delivery of ARPC's enterprise-wide security awareness and training program, building a strong security culture across all levels of the organisation.
  - Oversee implementation of ongoing education initiatives — including phishing simulations, targeted learning campaigns, and behavioural reinforcement — to strengthen cyber resilience.
  - Ensure all employees understand and fulfil their security responsibilities, particularly regarding safe use of AI tools, information classification, and secure data handling practices.
  - Embed security awareness into onboarding, learning programs, and continuous capability development
- **Efficiency & Cost Optimisation**
  - Rationalise and optimise security tools, platforms, and licensing to reduce duplication and maximise value.
  - Ensure all security investments are proportionate to ARPC's risk profile, deliver measurable risk reduction, and support business outcomes
- **Reporting & Visibility**
  - Maintain clear, data-driven dashboards and reports for executive and Board assurance, covering cyber risk, control effectiveness, and compliance status.
  - Provide visibility into emerging areas such as AI-related security metrics, third-party risks, and Zero Trust maturity.
- **Owns vendor governance for security-specific providers, including:**
  - Own governance of all security-specific vendors and service providers, ensuring performance, compliance, and value-for-money outcomes.
  - Oversee Managed SOC/SIEM services for 24/7 monitoring, detection, and escalation.
  - Manage penetration testing, vulnerability management, and threat intelligence partners.
  - Coordinate with providers of security awareness and training to ensure alignment with ARPC's learning and resilience objectives.
- **Other**
  - Lead or contribute to ARPC-wide corporate projects and strategic initiatives as required, supporting organisational priorities beyond the Information Security function.
  - Provide coverage for Senior Executive positions as required

Working relationships (key stakeholders, clients, customers, suppliers, providers, consultants, etc.)

Build and maintain strong relationships within:

- **Internal**
  - Build and maintain strong, collaborative relationships across all levels of ARPC to embed a culture of shared responsibility for information security.
  - Provide trusted advice and guidance to the Executive and Board on cyber security risks, trends, and assurance
- **External**
  - Develop and sustain productive partnerships with key vendors, service providers, and Government security agencies to enhance ARPC's security posture and resilience

Person specification

Qualifications and experience

Qualifications (indicate whether mandatory or desired)

- Degree in Information Technology, Cyber Security, or a related discipline **– Mandatory**
- Recognised industry certification in Information or Cyber Security (e.g. CISSP, CISM, CISA, or equivalent) **– Mandatory**
- Certification or formal training in Risk Management, Governance, or IT Service Management (e.g. ISO 27001 Lead Implementer/Auditor, COBIT, ITIL) – **Mandatory**
- Active security clearance or the ability to obtain and maintain an Australian Government security clearance – **Mandatory**

Experience (minimum type and level of experience required to perform the role)

- Demonstrated experience preparing and presenting formal cyber security or risk reports to Boards or Board Committees, with the ability to translate technical and risk concepts into clear, business-relevant insights – **Mandatory**
- Demonstrated experience leading enterprise cyber security functions, including strategy, implementation, compliance, and incident response **Mandatory**
- Strong understanding of the Australian Government's Protective Security Policy Framework (PSPF) and relevant information security standards such as Information Security Manual (ISM), and Essential Eight maturity model. **Mandatory**
- Proven ability to design and embed security governance, controls, and risk management practices across a cloud-first organisation. **Mandatory**
- Experience partnering with third-party vendors and managed service providers to deliver and assure security services and solutions — **Mandatory**
- Exceptional communication, influence, and stakeholder engagement skills, including at executive and Board levels – **Highly Desired**
- Experience leading organisational uplift in security culture, awareness, and capability — **Mandatory**

Key legislative / regulatory role responsibilities

Public Interest Disclosure Act 2013 (PID Act)

- ARPC staff must assist the ARPC CEO (or delegate) and/ or the Commonwealth Ombudsman in the conduct of a PID investigation.

Privacy Act 1988

- ARPC staff must adhere to the Australian Privacy Principles and the ARPC Privacy Policy and report any privacy breaches by any employee or contractor to the Privacy Officer / or Privacy Champion, as soon as they become aware of them.

Freedom of Information Act 1982 (FOI Act)

- ARPC staff are responsible for notifying and supporting the Information Public Scheme (IPS) Team to ensure published website Information is accurate, up-to-date and complete.
- ARPC 'owners' of website content are required to review content on their page(s) at least annually.

Work Health & Safety Act 2011 (WHS Act)

- All workers, including senior managers and executives, have duties under WHS Act.
- These duties include taking reasonable care for our own psychological and physical health and safety and that your actions or omissions do not adversely affect the health and safety of other persons.

Technical capabilities (skills, knowledge, technical or specialist capabilities)

- **Cyber Security Governance and Frameworks:** In-depth knowledge of the Protective Security Policy Framework (PSPF), Information Security Manual (ISM), Essential Eight, and related government standards.
- **Cloud Security (Microsoft Azure):** Strong understanding of cloud security architecture, identity and access management (IAM), endpoint protection, and secure configuration principles in an Azure environment.
- **Security Risk and Assurance Management:** Skilled in identifying, assessing, and managing cyber risks; maintaining control libraries; and providing assurance to executive and board stakeholders.
- **Incident Response and Threat Management:** Experience overseeing incident detection, response, and recovery processes, including coordination with managed SOC/SIEM providers.
- **Enterprise Security Platforms:** Proficiency in platforms including Microsoft Defender for Endpoint and Cloud, Zscaler for secure access and zero trust, and Azure Sentinel for advanced SIEM detection and response.
- **Data Protection and Privacy:** Knowledge of data governance, information classification, data loss prevention (DLP), and compliance with the Privacy Act and APS data management standards.
- **AI and Emerging Technology Risk:** Awareness of security, ethical, and governance considerations for the adoption of AI tools and data analytics platforms (e.g. Databricks).
- **Reporting and Analytics:** Ability to interpret and present complex security data through dashboards and reports ideally leveraging Power BI to inform decision-making and communicate risk posture.
- **Vendor and Contract Management:** Capability to manage and assure security outcomes through third-party vendors, managed service providers, and external auditors.
- **Continuous Improvement and Maturity Uplift:** Competence in developing and applying maturity models, performance metrics, and improvement roadmaps to drive organisational resilience.
- **Sound Judgement and Legislative Acumen:** Demonstrates strong capability in interpreting and applying legislation, regulatory obligations, and policy frameworks relevant to ARPC's operating environment.
- **Insight and Innovation:** Naturally curious and improvement-focused, seeking opportunities to enhance security effectiveness, efficiency, and organisational resilience through insight, initiative, and innovation.
- **Attention to Detail:** Maintains a high level of accuracy and diligence in reviewing technical, risk, and compliance information, ensuring quality and reliability of outcomes.
- **Collaborative Leadership:** Works effectively both independently and as part of a cross functional teams; acts as a trusted subject matter expert and partner across business and technology domains.
- **Professional Presence and Courteous Assertiveness:** Communicates with clarity, confidence, and respectable to influence outcomes and maintains strong relationships with internal and external stakeholders

Authorities	**Limits/ type**
Financial delegations:	As per ARPC Delegations Policy
HR delegations:	As per ARPC Enterprise Agreement
Declared Terrorist Incident (DTI) and Declared Cyclone Event (DCE):	As per ARPC Event Response Policy

ARPC Values			
• Integrity	• Respect	• Service	• Wellbeing

ARPC Capabilities (Integrated Leadership System)

ARPC Capabilities describe behavioural expectations for all employees, by classification broadband.

- Shapes strategic thinking
- Achieves results
- Supports/cultivates productive working relationships
- Displays/exemplifies personal drive and integrity
- Communicates with influence

Prepared by: *(Name & Position)*	Sachin Nadgauda Head of IT	**Date:**	October 2025
Endorsed by: *(Name & Position)*	Victoria Simpson COO	**Date:**	October 2025
Approved by: *(Name & position)*	Chris Wallace CEO	**Date:**	October 2025