ARPC Position Description

Role title:	Information Security Analyst		
Function:	Information Security	**Classification broadband:**	ARPC5/6
Location:	Sydney	**Security clearance:**	Baseline
Role reports to:	Head of Information Security		
Direct reports:	nil		

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

Reporting to the Head of Information Security and working closely with the Cyber Security Manager, the Information Security Analyst supports ARPC's cyber security operations through monitoring, analysis, and reporting. The role provides timely insights and data to enable informed decisions, strengthen incident response, provides hands-on technical support to maintain M365 security environment and maintain visibility of ARPC's overall security posture

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

Monitoring & detection

- Monitor and review security alerts and events from ARPC's managed SOC and internal systems.
- Conduct initial triage of security incidents and escalate to the Cyber Security Manager as required.
- Maintain and improve ARPC's Microsoft 365 Secure Score, ensuring continuous alignment with best practices and organisational risk posture.
- Administer and monitor Microsoft Defender products (Defender for Endpoint, Defender for Identity, Defender for Office 365, and Defender for Cloud Apps) to detect, investigate, and respond to threats in coordination with the Cyber Security Manager and SOC provider.
- Manage and optimise Microsoft Sentinel, including log ingestion, data connectors, analytics rules, playbooks, and dashboard tuning to enhance detection and response capabilities.
- Assist in improving alert accuracy in collaboration with managed service providers.

Dashboards & reporting (Power BI)

- Design, develop, and maintain dashboards to visualise cyber risk, control effectiveness, and incident trends.
- Track vulnerability status and remediation progress, ensuring data accuracy and visibility.
- Automate and streamline reporting processes to improve efficiency and timeliness.
- Prepare operational reporting for the Head of Information Security and contribute to Management and Board-level reporting packs.

Assurance & continuous Improvement

- Support the maintenance of cyber security metrics, registers, and control libraries.
- Assist in identifying opportunities to improve monitoring, detection, and reporting processes.
- Contribute to initiatives that enhance ARPC's cyber resilience and data-driven decision-making.

Collaboration & support

- Work closely with the Cyber Security Manager and Technology Team to coordinate response activities and share insights.
- Support awareness and training initiatives by providing data and insights on phishing, incidents, and user behaviour.
- Maintain accurate documentation of security monitoring and reporting processes.

Risk capability

- Actively contribute to managing risk well at ARPC by embedding risk into day-to-day activities supporting a culture of openness, accountability and continuous improvement.

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

Internal

- Reports to the **Head of Information Security** and works closely with the **Cyber Security Manager** for day-to-day direction and guidance.
- Collaborates with the **Technology and Transformation Team** to support incident response, vulnerability management, and security control improvement.

- Partners with the **Risk and Compliance Team** to align monitoring and reporting with ARPC's enterprise risk frameworks.

External

- Supports vendor relationships by providing operational input into security reporting and assurance activities.

May liaise with other external partners or agencies as directed by the Head of Information Security

Person specification

Qualifications (indicate whether mandatory or desired)

- Tertiary qualifications in Information Technology, Cyber Security, Data Analytics, or a related discipline — ***Desired***
- Industry certification or training in information security, risk, or data analytics (e.g., CompTIA Security+, Microsoft Certified: Security, Compliance & Identity Fundamentals, or equivalent) — ***Desired***
- Ability and willingness to undertake relevant cyber security or data analytics training as part of professional development — ***Mandatory***

Experience requirements

- Experience in a technology, data, or analytical role with exposure to security operations, reporting, or risk management — ***Desired***
- Strong analytical skills with the ability to interpret data, identify patterns, and communicate insights clearly — ***Mandatory***
- Demonstrated curiosity and initiative to learn about cyber security, cloud technologies, and data-driven reporting — ***Mandatory***
- Experience using tools such as Power BI or similar platforms for data visualisation and reporting — ***Desired***
- Experience working collaboratively across teams or with external service providers in a technical or risk-focused environment — ***Desired***

Key legislative / regulatory role responsibilities

Comply with the Public Interest Disclosure Act, Privacy Act, FOI Act, and WHS Act and support ARPC's security and governance protocols.

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 and/ 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 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.

Security

- Responsible for monitoring their staff (including contractors), resources and functions to ensure security controls are maintained and operate effectively.
- Responsible to ensure that staff (including contractors) are aware of and practice the appropriate security procedures for protecting individuals, official information and other valuable resources.

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)

- **Microsoft Environment:**
  Strong working knowledge of Microsoft 365 applications and tools, including Power BI, Excel, Word, and PowerPoint, with the ability to create clear, insightful reports and visualisations.
- **Operational Security Tools Management:**
  Experience with Microsoft Defender, Sentinel, and related Microsoft 365 security products for monitoring and incident response.
- **Cyber and Information Security Awareness:**
  Foundational understanding or keen interest in information security principles, with the ability to apply sound judgment in handling data, incidents, and risk information.
- **Collaboration and Stakeholder Engagement:**
  Strong interpersonal skills with the ability to collaborate effectively across teams and build trusted working relationships with internal and external stakeholders.
- **Communication:**
  Excellent written and verbal communication skills, capable of translating technical or analytical information into clear, concise messages for diverse audiences.
- **Problem-Solving:**
  Practical approach to problem-solving, demonstrating initiative, curiosity, and a commitment to continuous improvement in monitoring, reporting, and data quality.
- **Attention to Detail:**
  Attention to detail ensuring accuracy, accountability, and professionalism in all interactions and outputs.

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

Additional requirements

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

Refer to ARPC’s intranet for detailed information on each of the capability areas.

Prepared by:	Jarod Inzitari Interim, Head of Information Security	**Date:**	28 November 2025
Approved by:	Victoria Simpson Chief Operating Officer	**Date:**	28 November 2025