Role Description

General information

Title:	Senior ICT Security and Risk Specialist			**Classification:**	ASO7
Division:	Corporate	**Branch:**	Information and Communication Technology	**Business Unit:**	ICT Information Governance & Security
Type of Appointment:	Term/Ongoing	**Hours of Duty:**	37.5	**Location:**	Adelaide

About Us

South Australia is internationally recognised for the quality of its agriculture, food and wine. Our regions are the backbone of our state and the economic powerhouse that drives prosperity for all South Australians.

The Department of Primary Industries and Regions (PIRSA) is a key economic development agency working in partnership with our primary industries, regional stakeholders and across all levels of government to advance the prosperity and sustainability of South Australia's primary industries and regional communities.

We are a passionate team of around 800 people working across metropolitan and regional South Australia to develop and protect our state's regions and food, wine, aquaculture, fisheries, forestry, grains, livestock, dairy and horticulture industries.

Purpose

The primary purpose of the role is to lead the PIRSA cyber security program, including risk management, policy development and compliance and security activities.

The role contributes delivering the agency's priorities including organisational performance as a modern, flexible and responsive organisation that values and develops its people.

The role contributes to delivering Corporate Services directions including providing an efficient, reliable and secure ICT environment that supports PIRSA in delivering services to its customers and takes advantage of new technologies to enable improvements in the way the agency operates.

Key Accountabilities

- Provides expert strategic and technical advice in relation to cyber security.
- Leads the development and management of the cyber resilience maturity roadmap and initiative implementation.
- Researches and prototypes new technologies and contribute to projects and business activities in a specialist cyber security capacity.
- Leads the development, implementation and continuous improvement of information security management policy and process.
- Ensure adequate development and maintenance of ICT security documentation.
- Lead security awareness and ICT support strategies.
- Ensure PIRSA compliance with Whole of Government ICT Security standards.
- Promotes and leads ICT security quality assurance and audit functions.
- Ensures appropriate capabilities are maintained to monitor system security events for security incidents and policy breaches and respond to them in accordance with the policies, standards and procedures defined in the ISMS.
- Performs the Information Technology Security Adviser (ITSA) role.

Key Deliverables / Results

- Effective security and risk strategies and roadmaps are developed that increase PIRSA's cyber security resilience.
- Security management policies and processes are developed to ensure the integrity of the PIRSA ICT environment.
- New technologies are researched and prototyped which enhance PIRSA's ICT resilience.
- Leadership is provided in ICT in the areas of ICT security and risk, including convening the PIRSA ICT Security Forum.
- PIRSA staff are educated so that they understand and comply with agency and whole of

Role Description

• PIRSA's ICT Disaster Recovery capability is managed and continually improved. • Cyber threats are detected, investigated and resolved. • Efficient and accurate measurement, monitoring and reporting mechanisms are developed for cyber threats.	government ICT policies and standards. • Risk Management practices are integrated effectively into all ICT functions.

Relationships

• Reports to Manager Information Governance & ICT Security. • Provides advice and guidance to the IT security Analyst. • Engages with security and risk specialists across SA Government and builds strong relationships with the Office of Cyber Security in the Department for Premier and Cabinet.	• Represents PIRSA on relevant whole of government committees. • Works closely with Senior Management and staff across PIRSA. • Liaises regularly and proactively with ICT service providers.

Requirements

- Out of hours work and inter / intrastate travel may be required.
- Australian residency or current works permit is required (responsibility of applicant to provide evidence of a current work permit).
- You acknowledge your work, health and safety obligations and our expectations.

Qualifications

- Essential: A valid certification to an internationally recognised information security standard.
- Desirable: A relevant tertiary qualifications in ICT.

Capabilities

Capability	Behaviours
Professional & Technical Knowledge Demonstrates an in-depth knowledge across all key areas of professional competence relevant to the role, with expert knowledge in ICT security and risk management	• Expert knowledge of the risk management framework and its application to support a sustainable and secure network environment. • Experience in developing and implementing best practice ICT security standards, guidelines and policies and in monitoring compliance to these standards. • Experience in developing and implementing best practice tools and fixes to ensure the integrity of IT networks and systems. • Experience in monitoring ICT networks for security breaches and investigating violations when they occur. • Demonstrated ability to provide solid recommendations and advice to management regarding ICT security to support decision making. • Strong analytical skills and the ability to recognise trends with limited evidence and develop creative solutions to ICT problems and issues. • Possesses strong understanding of current cyber security trends. • Expert knowledge of the South Australian Government Cyber Security Framework, Protective Security Management Framework and AS/NZS IS/IEC 27001:2006 and 3100:2009 standards.
Risk Management Plans and implements organisation-wide processes and procedures for the management of risk to the success or	• Carries out risk assessment within a defined functional or technical area of business. • Uses consistent processes for identifying potential risk events, quantifying and documenting the probability of occurrence and the impact on the business. • Refers to domain experts for guidance on specialised areas of risk, such as architecture and environment. • Co-ordinates the development of countermeasures and contingency plans.

Role Description

integrity of the enterprise.	
Security Administration Provides operational security management and administrative services. Typically includes the authorisation and monitoring of access to IT facilities or infrastructure, the investigation of unauthorised access and compliance with relevant legislation.	• Drafts and maintains the policy, standards, procedures and documentation for security. • Monitors the application and compliance of security operations procedures and reviews information systems for actual or potential breaches in security. • Ensures that all identified breaches in security are promptly and thoroughly investigated. • Ensures that any system changes required to maintain security are implemented, and that security records are accurate and complete.
Information Security Defines and operates a framework of security controls and security management strategies.	• Obtains and acts on vulnerability information and conducts security risk assessments for business applications and computer installations; provides authoritative advice and guidance on security strategies to manage the identified risk. • Investigates major breaches of security and recommends appropriate control improvements. • Interprets security policy and contributes to development of standards and guidelines that comply with this, and ensures proportionate response to vulnerability information, including appropriate use of forensics. • Performs risk assessment, business impact analysis and accreditation for all major information systems within the organisation.
Problem Management Manages the life cycle of all problems that have occurred or could occur in delivering a service.	• Ensures that appropriate action is taken to anticipate, investigate and resolve problems in systems and services. • Ensures that such problems are fully documented within the relevant reporting system(s). • Coordinates the implementation of agreed remedies and preventative measures. Analyses patterns and trends.

HRMS No:	P19641/P19660	**ANZCO Code:**		**Objective ID:**	
Delegate Approval:	Michelle Griffiths, Executive Director			**Date:**	August 2022
Approved and Classified by People and Culture:	August 2022				