



## General Manager – Information Governance & Security (CISO) (Digital Business Solutions)

### About RSL Queensland

RSL Queensland is a dynamic, forward-thinking social purpose organisation, developing and delivering innovative programs that build brighter lives for Australia's Defence Family. Augmenting our diverse network of Sub Branches, we're leveraging new research and data to create innovative, next-gen services and delivery hubs, reinvent traditional commemorations for the digital age, and provide a strong policy voice on behalf of all generations of veterans.

### Our Purpose:

Our purpose is to support a bright future and enduring legacy for all veterans and their families. For more than one hundred years we have worked to protect the rights of those who have sacrificed so that we may live peacefully, and this continues to drive us today. With this in mind, our goals for the future are clear:

- Transform the lives of veterans so that their average quality of life matches that of the general population
- Become the leading voice representing the interests of the Australian Defence Community and the Ex-Service Organisation community as a whole
- Continue to grow a sustainable business that enables both relevance and influence to flourish

### What we do:

Our support programs include: veteran and partner employment, employer education, advocacy, health and well-being, education and scholarships, counselling, homelessness assistance and crisis care. Through medical research grants and partnership development programs, we are pioneering an outcomes-oriented, holistic approach to improving the defence family's quality of life. Funding our community work are our prize home lotteries, Australia's largest and most successful not-for-profit art union.

## About Digital Business Solutions at RSL Queensland

DBS works to safeguard RSL Queensland from cyber-attacks and ensures we're using the best tech to enhance our communication and capability while setting up all team members with the technical tools and support they need to thrive.

DBS comprises five business units: Engineering & Operations; Digital Engagement; Enterprise Digital Solutions; Digital Strategy, Improvement & Security; and Digital Planning & Performance.

DBS's capabilities span architecture, digital engagement and delivery, information security, data governance, and technology services including software engineering, automation and operations – all of which underpin and enable our services to the Veteran community, and the Art Union Prize Home Lottery.

### Role Purpose:

The General Manager of Information Governance & Security (CISO) will be accountable for preparing and implementing information security and governance strategies that improve the productivity and profitability of RSLQ. The General Manager will govern business unit planning, workforce & talent management, continual improvement, service level management and reporting for DBS. The General Manager will act as RSL Queensland's Chief Information Security Officer.

This role leads RSLQ's information and data architecture's creation, iteration, and maintenance, embodying the fundamental principles that describe RSLQ's future state and enable its evolution. This work involves the interpretation of business goals and drivers, the translation of business strategy and objectives, the strategic assessment of current capabilities and the identification of required changes in information security and governance capabilities.

The role also leads the enterprise architecture team, responsible for creation, iteration, and maintenance, embodying fundamental principles that describe RSLQ's digital and ICT future state and enable its evolution.

They will be responsible and accountable for providing strategic-level guidance for the organisation's information & cyber security program and ensuring compliance with information & cyber security policy, standards, regulations, and legislation.

### Key Accountabilities:

This role will report to the **Executive General Manager – Digital Business Solutions (CIO)** and is accountable for leading the **Information Governance & Security** team. Key responsibilities of the position include:

### Service Delivery

#### *Service Delivery Leadership*

- Deliver, review and improve RSL Queensland's Security Strategy and Roadmap to create a comprehensive, resilient, evolving and adaptive security operating environment for the organisation.
- Lead the information and security implementation of the organisation's strategic initiatives, projects and/or the establishment of new capabilities or services.
- Recommend and oversee the initiatives that develop and enhance an information security management framework.

- Understand and interact with related disciplines through Board and Board Committees, Executive and Leadership committees to ensure the consistent application of policies and standards across all technology projects, systems, and services.
- Provide leadership to the enterprise's information security portfolio, maintaining confidentiality, integrity, and availability across the domains of people, process and technology.
- Assist with the overall business technology planning, providing a current knowledge and future vision of technology, systems and capability gaps.
- Act as a thought leader continually communicating their information security and governance strategy and vision.
- Provide appropriate team structure, support and guidance to team members to ensure acceptable delivery from all Information Security & Data Governance staff and fostering a culture of expertise development and uplift of organisational skills.
- Ensure team knowledge of legislations, relevant issues and community trends is kept up-to-date and current through formal knowledge sharing activities, coaching/mentoring and formal training.
- Oversee the development of policies, procedures and controls of operating activities to ensure the achievement of objectives and mitigation of organisational and technology risks.
- Oversee the delivery and operational management of information security responsibilities such as Digital Forensics and Incident Response, Cyber Threat Intelligence, Vulnerability Management, Continuous Monitoring and Information Security Reporting.

#### *Security Architecture*

- Work in partnership with DBS leaders especially Enterprise Architecture to ensure that the organisation's needs for Data Security, Platform Security and Technology Infrastructure Resilience are designed, implemented and managed.

#### *Awareness & Training*

- Oversee the development and implementation of cybersecurity awareness and training aligned to the organisation's goals and regulatory requirements.
- Oversee the design and execution of security awareness programs
- Establish metrics and feedback loops to measure the effectiveness of the awareness and training programs, making necessary adjustments based on data.

#### *Incident Management*

- Establish and oversee the cyber incident management strategy and framework, ensuring it aligns with the organisation's risk appetite and regulatory landscape.
- Lead and coordinate a cross functional cyber incident response team including managed service providers, ensuring timely and effective response to security incidents. Act as the interface between incident response teams and organisation's executive.
- Ensure thorough post incident analysis is conducted after each incident, including root cause analysis, to prevent future occurrences.

#### *Incident Response Reporting & Communication*

- Design and implement a communication strategy for incidents, ensuring transparent and timely updates to relevant stakeholders, including top management, board members, regulators, and, when appropriate, the public.

- Liaise with Marketing, Legal, and relevant departments to ensure communications are consistent, accurate, and adhere to regulatory and legal requirements.
- Build and maintain relationships with external stakeholders, such as law enforcement, other CISOs, and industry groups, for sharing threat intelligence and best practices.

#### *Incident Recovery Plan Execution*

- Develop, maintain, and oversee the execution of a comprehensive incident recovery plan, ensuring the rapid restoration of IT systems and business operations.
- Ensure the regular test of the recovery plan, using realistic scenarios, to ensure its effectiveness and relevance.
- Ensure close alignment between the incident recovery plan and the broader business continuity and disaster recovery strategies.
- Update the recovery plan based on lessons learned from incidents, drills, and changes in the IT environment or business operations.

#### *IT Disaster Recovery Management*

- Develop and maintain DBS's IT Disaster Recovery Management in line with RSL Queensland's Business Continuity Plans. This includes, and is not limited to, preparing and updating plans for business continuity and disaster recovery in the event the company is the subject of a cyberattack.

### **Financial**

- This position has financial delegations as per the Delegations of Authority policy and provides support to the **Executive General Manager – Digital Business Solutions (CIO)** to drive achievement of financial management targets.
- Ensures all finance-related activities are conducted in a manner aligned to RSL Queensland policies and procedures
- Leads achievement of financial management targets as set up Executive and Senior Leadership
- This position is classified as a T-3 position and holds the associated delegated authority as per the [Delegations of Authority policy](#) and the [Sub Delegations Matrix](#).

### **Workforce**

- This position will be responsible for leading a team of professionals and will provide support to the **Executive General Manager – Digital Business Solutions (CIO)** to drive achievement of workforce management targets.
- Collaborates and interlocks effectively with other teams across RSL Queensland and its League network.
- Personally contributes to a culture of positive organisational engagement, creativity, experimentation and innovation within the team.
- Develops KPIs for self and direct reports as cascaded from Executive Leadership to fulfil annual organisation goals and objectives and participates in performance management programs as required by the organisation.
- Develops an annual Individual Development Plan (IDP) to continuously evolve skills and expertise.
- Supports and enables direct reports to develop an annual Individual Development Plan (IDP) to continuously evolve skills and expertise
- Ensures participation for self and direct reports in organisational training and engagement surveys as required

- Ensures self and team compliance with People & Culture, Workplace Health and Safety Management and other relevant policies and procedures ongoing
- Implement documented procedures for hazard identification and WHSW risk management and ensure that workers, including volunteers and contractors, abide by all WHSW procedures.

## Qualifications and Experience:

### Mandatory

- Tertiary degree in business management or a technology-related field required or demonstrable equivalent experience.
- 10+ years' experience leading and operating within a diverse range of technical and specialist teams in high-performing environment including inhouse staff and external service providers.
- Sound knowledge and demonstrated experience in the application of common information security management standards and compliance frameworks, such as ISO/IEC 27001, PCI DSS, Australian Privacy Act, GDPR, NIST and the M1TRE Attack Framework.
- Demonstrated understanding of current legislation relating to cyber and information security, including the Privacy and Data Protection Act 2014.
- Demonstrated experience in leading risk management processes and the ability to communicate complex technical risks in terms of business impact using easy to understand language
- Innovative thinking and leadership with an ability to lead and motivate cross-functional, interdisciplinary teams.
- Knowledge of modern IT systems and security architecture.
- Proven track record in developing and leading information/cyber strategy (development and implementation), including the ability to distil and articulate complex issues and remediation proposals.
- Highly developed relationship building and stakeholder management skills, demonstrated ability to bring all cohorts, stakeholders and service providers along the journey in a positive manner, high emotional intelligence, and strong stakeholder management skills.
- Demonstrated strong verbal, written, interpersonal, negotiation, networking, partnering and relationship management skills. Competent in executive level communications and collaboration.
- The proven ability to manage competing priorities, work collaboratively across the department, and ensure a positive collaborative working environment for the DBS team.

### Preferred

- Post graduate qualifications in business management or a technology-related field.
- Certifications including CISSP (Certified Information Security Systems Professional) or CISM (Certified Information Security Manager).
- Good knowledge of information or data architecture
- Experience and leadership in setting targets, budgets and monitoring and measuring performance.
- Well-developed research, analytical and problem-solving skills, including the ability to gather and compile information to develop reports and maintain databases.
- Experience in Agile (scaled) software development or other best in class development practices.
- Experience with contract and vendor negotiations and management including managed services.
- Experience working in industry sectors such as Defence, Emergency Services or Not-for-Profit.

## Demonstrated Capabilities:

### Strategic thinking:

- Influence the organisation's strategic response to business priorities.
- Articulates and champions vision and strategic agenda (2030 Strategy) leading and encouraging inputs to drive strategy across the organisation.
- Engage in high-level business analysis to formulate effective, long-term workforce responses to critical business priorities.
- Think laterally and integrates considerations from across the Organisation when reaching decisions and making recommendations.

### Achieving Results

- Direct the development of effective systems for the establishment and measurement of accountabilities and evaluate ongoing effectiveness.
- Ensure that legislative and regulatory frameworks are applied consistently and effectively across the organisation.
- Create a culture of achievement fostering on-time and on-budget quality outcomes in the organisation.
- Inspire a culture which respects the obligation to manage public monies and other resources responsibly and with probity.
- Build staff support and commitment to announced change, and plan and prepare for long-term organisational change, with a focus on the wider political, social and environmental context.
- Ensure organisational compliance with WHS legislation and encourage a proactive WHSW risk management approach across the organisation.

### Communicating with Influence

- Champion the organisational vision and strategy and communicate the way forward.
- Accurately assesses communication trends and nuances within the organisation and acts to meet emerging needs for communication and change management.
- Engage in a range of approaches to generate solutions, seeking expert inputs and advice to inform negotiating strategy.
- Actively promotes a healthy climate of communication, including information handling, sharing and goal alignment.
- Use own professional knowledge and expertise of others to drive organisational objectives forward.

### Effective Teamwork

- Establish a culture and supporting systems that facilitate information sharing, communication and learning across the sector.
- Seek out and facilitate opportunities to engage and collaborate with stakeholders to develop organisational, cross-jurisdictional and departmental solutions.
- Identify and overcome barriers to collaboration with internal and external stakeholders.
- Builds positive relationships with key stakeholders across the business and externally to achieve positive business results.

### Other information:

- RSL Queensland is an equal opportunity employer and is committed to providing a safe and healthy work environment free from discrimination, harassment, or bullying
- Our values drive us. They support communication and values-based behaviours within teams. Alignment to our values is a key factor for success at RSL Queensland

- 
- RSL Queensland is committed to employing from within the Defence sector where possible
  - Inter and intra state travel may be required