Role Statement

Position title: Chief Information Security Officer (CISO)

Position number: 40001560

Salary and Level: Level 8 PCSCAA 2022

Reports to: Chief Information Officer (CIO)
Direct reports: Nil

The organisation

Lotterywest is the only State Government owned and operated lottery in Australia, where all the available profit is returned to the Western Australian Community through discretionary and statutory grants. Lotterywest has supported the Western Australian community for over 90 years. Its vision for 'a hopeful, health, connected and sustainable community life for all Western Australians'.

Lotterywest is the employing agency for Healthway, which is the only State Government agency dedicated to health promotion. For over 30 years Healthway has been providing grant funding to sport, arts and racing organisations, community activities, and to health promotion projects and research. Healthway's vision is for a 'healthy and more active Western Australia.'

About the business unit

Technology Services is responsible for the technology services and support IT functions across all areas of the Lotterywest and Healthway businesses. The area is also responsible for the overarching compliance, change management and technology partner services for Lotterywest gaming and Lotterywest and Healthway grant management systems. In doing its work, the Technology Services team works collaboratively across the organisation to ensure technology business needs are met.

The business unit is undertaking transformation in the way it delivers services, consistent with the Board endorsed strategic direction. This is with the purpose to deliver an agile, scalable, responsive team and digital business operating model, including investment in cloud services, focused strategic vendor management and contemporary digital solutions to deliver on current and future business outcomes.

Key focus areas of the position

The Lotterywest Board identified cyber security as a significant strategic risk facing the organisation.

Reporting to the Chief Information Officer (CIO) and working directly with other Executives as required, this role oversees information/cyber security risk management and is responsible for the development of Lotterywest's information/cyber security culture and resilience.

Role Statement

The role seeks to develop and maintain technologically current, highly integrated and secure security architecture and secure business practices. The role involves scoping, designing, evaluating, and reviewing end-to-end security solutions and working closely with Lotterywest's Technical Services function and the Cybersecurity team under Strategy and Enablement, to prioritise and deliver technical security initiatives.

The role has the following key areas of focus:
- System security - Developing, implementing, monitoring, and reviewing information security strategy, solutions and practices, to mitigate risk and support good practice.
- Risk management - Ensuring the assets and information of Lotterywest are appropriately secured at all times by identifying areas of security risks and addressing areas of exposure.
- Compliance – Monitoring, reviewing, enforcing and reporting compliance with information security strategies and practices to ensure desired security standards are being met.
- Governance - Oversight of system security governance and business operating practices, investigation of security breaches and meeting government security reporting obligations.

Key responsibilities
Directs development, implementation, delivery and support of the enterprise information/cyber security strategy
- Plans, develops and drives cyber security strategies in line with business requirements and in alignment to and integrated with enterprise architecture
- Determines and oversees the roadmap of activities for the overall cyber security strategy
- Undertakes research to identify information security opportunities and industry best practice

- Develops and reviews information security related policies, processes, plans and procedures, ensure security and governance practices align with the organisation's objectives.
- Is the escalation point for major security events and incidents and produces monthly reporting for CIO and Executive team

- Ensure that the WLA (World Lottery Association) standards, framework and Audits are maintained at the highest standard to meet Lotterywest regulatory obligation
- Identify and assess security risks within the organisation in real time and implement security measures to mitigate risks
- Ensure compliance with relevant laws, regulations, and industry standards related to data security and privacy
- Educate staff in the organisation on the best IT practices and regulatory requirements
- Work closely with other high-level executives to develop all-encompassing security strategies
- Stay up-to-date with the latest security threats and best practices, and adapt the company's security strategy accordingly

Role Statement

Ensures governance and compliance between business strategies and information security
- Maintains accreditations under the Essential 8, World Lottery Association (WLA) and the ISO27001 Information Security Management System (ISMS)
- Plans, organises and leads the information/cyber security programme and initiatives
- Chairs the Security Committee and supports the Audit Risk Management Committee on all security matters and incidents
- Develops a strong security culture through training, communication and promotion of security awareness in line with identified information/cyber security risks
- Works with internal testing/audit staff, and consultants on required security assessments such as vulnerability assessments and penetration testing
- Maintains engagement with DGOV (Office of Digital Government) and other relevant Government Authorities ensuring that Lotterywest is visible and receiving the latest security strategy, policy and technical updates.

Leads provision of information/cyber security expertise, guidance and systems
- Provides expert knowledge and leadership in setting clear, achievable and proportionate direction/plans for information/cyber security
- Clearly articulates the relevant metrics of the information/cyber security posture to the executive and Audit Risk Management Committee
- Provides expertise, direction, guidance and assistance responding to critical information/cyber incidents, disaster recovery and business continuity
- Works collaboratively with other business units and project managers to ensure information/cyber security considerations are recognised and addressed during planning and implementation of all initiatives
- Advises on security implications of system architecture design and changes
- Makes recommendations regarding the security requirements for the development, modification and testing of information, projects, business systems, infrastructure and game processes
- Undertakes strategic information/cyber security coordination with external stakeholders
- Provide guidance and support for projects and major undertakings to ensure correct security architecture, protocols and policies are embedded.

Secures organisational resources to execute the information/cyber security strategy.
- Provides leadership and direction to the Security Team, which is responsible for detecting and assessing and addressing information/cyber security threats and vulnerabilities
- Contributes to relevant risk management assessments and performs information/cyber vulnerability, threat and risk analysis and development/execution of treatment plans
- Ensures appropriate security controls are in place and monitored across all information systems
- Undertakes incident response planning, testing and responding
- Investigates information/cyber breaches or incidents, and offers rectification recommendations
- Prepares and presents comprehensive reports on information/cyber security performance
- Assists with audit assurance and compliance activities regarding information/cyber security matters and the remediation of findings

Role Statement

- Capacity to match security projects to corporate objectives.
- Manages third party security vendor service and contracts, reviews service and product offerings regularly to ensure relevance and best ROI.
- Meets all internal and external reporting obligations

Other
- Other duties as required

Mandatory / special role requirements
- Drivers licence / Police Clearance / After-hours work

Essential selection criteria
1. Extensive experience in technical information/cyber security analysis, governance and risk management
2. Demonstrated knowledge of information/cyber security architecture and security testing
3. Experience in ISMS and knowledge of ISO/IEC 27001 Standard, NIST,PCI DSS and the Essential 8 framework.
4. Demonstrated high level ability to work collaboratively across teams
5. Demonstrated high level experience developing and managing relationships with internal and external customers, business partners and stakeholders
6. Demonstrated high level communication skills including the ability to build trust and influence

Required Qualification

This role requires possession of a relevant tertiary qualification and/or at least 5 years' experience managing an information/cyber security function for a comparable organisation.

Authorised by:

Caroline Niewiarowski-Fish
Chief Information Officer
Date: 6 December 2024