Chief Information Security Officer

Position Description

Directorate:	Corporate Services
Reports to:	Chief Information Officer
Direct reports:	NIL
Location:	Flexible within any of the Society's main metropolitan or regional offices across NSW.
Primary position objective:	Define and execute the cyber security strategy for the Society aligned to recognised standards and frameworks that drives a culture of risk management, awareness, capability, and supports greater resilience to cyber security threats. Ensure the Information Security governance, risk and compliance strategy and framework supports strategic objectives and meets audit, legal and risk mandates.

The St Vincent de Paul Society is an Equal Employment Opportunity Employer

Directorate overview

This position is in the Corporate Services directorate. The teams within the directorate and their functions are:

Strategy and Outcomes: this team is responsible for implementing a Society-wide planning, monitoring and reporting framework to support the achievement of the goals of the Strategic Plan; and leading the measurement of performance and outcomes of Society programs, services and functions.

Governance, Risk and Safeguarding: this team is responsible for supporting good governance practices throughout the Society; provision of State Council and Board secretariat services; leading the development of organisational policy; safeguarding functions; and enterprise risk management.

Legal: this team is responsible for delivering legal services, and privacy and complaints functions.

Policy and Advocacy: this team is responsible for developing informed public policy positions on issues relevant to the people we serve; directing relevant research; and developing and implementing related advocacy strategies.

People and Culture: this team is responsible for the Society's people related functions and strategy including people strategy; people policy; people systems; diversity and inclusion; organisational development; recruitment; workforce operations; employment relations and business partnering.

Information and Communication Technology: this team is responsible for state-wide ICT strategy; ICT project management; design and implementation of new ICT systems; ICT service desk, and cybersecurity.

Safety and Emergency Management: this team is responsible for state-wide work, health and safety strategy; work, health and safety audits; wellbeing; return to work and emergency management functions.

Accountabilities and responsibilities

The Chief Information Security Officer will:

- Ensure the successful implementation of the Strategic Plan within the Corporate Services directorate.
- Lead the development and implementation of cyber security strategies for the Society that enable stronger resilience to cyber security threats, ensuring that appropriate security technologies, architectures, policies and compliance frameworks are in place to protect the organisation's systems and information.
- Develop, implement and monitor a Technology Risk and Security Framework and program, in collaboration and consultation with appropriate stakeholders.
- Develop, implement and communicate, along with Technology management, a Disaster Recovery Plan that achieves the business continuity requirements of the organisation.
- Manage incident investigations, review and assess Technology controls to ensure ongoing effectiveness of policies, standards and control mechanisms.
- Implement policy and strategy for the selection of solution architecture components, and co-ordinate design activities, promoting the discipline to ensure consistency.
- Analyse organisational cyber security issues including gaps in governance, risk, audit and compliance strategies and practices and develop solutions to ensure business, statutory and legislative obligations and standards are met and the organisation is positioned to effectively respond to incidents..
- Design and communicate high-level structures to enable and guide the design and development of integrated solutions that meet current and future business needs.
- Provide advice on technical aspects of system development and integration (including requests for changes, deviations from specifications, etc) and ensures that relevant technical strategies, policies, standards and practices (including security) are applied correctly.
- Use appropriate tools, including logical models of components and interfaces, to contribute to the development of systems architectures in a specific business or functional areas.
- Provide authoritative advice, oversight and a single point of coordination to ensure the Society's cyber security risk, audit and compliance strategy is aligned with business objectives and is delivering measurable and appropriate value to all directorates within a known and acceptable level of risk.
- Assist in the preparation of technical plans within a business change programme and cooperate with Governance Risk and Safeguarding and project staff to ensure that appropriate technical resources are made available.
- Provide subject matter expertise and strategic domain architectural services within the cybersecurity practice domain, including End-point security management, Identity and Access Management, Vigilance and Resilience, Operational Technology.
- Develop and maintains enterprise security architecture for the organisation to ensure long term operation and affordability of the society's cyber security controls.
- Provide comprehensive guidance and oversight on the selection of, the development of, and

modifications to, security-related solution components to ensure that they take account of relevant architectures, strategies, policies, standards and practices (including security) and that existing and planned solution components remain compatible.

- Partner with the Technology Services management, teams, platforms and vendors to ensure a collaborative approach to implement best practice strategic initiatives and build cyber and digital capabilities and cyber security controls are implemented.
- Contribute to a safe working environment for members, staff and volunteers by implementing the Society's workplace health and safety practices.
- Contribute to the implementation of effective risk management procedures to ensure compliance with legal, employment and governance requirements.

Critical Key Performance Indicators (KPIs)

- NIST Cyber Security Maturity level.
- User cyber security awareness levels.

Key working relationships

In addition to the Chief Information Officer and their direct reports, the Chief Information Security Officer will foster close working relationships with:

- Executive Directors and Directors across the Society;
- Key users and vendors.

Essential criteria

Critical capabilities

There are nine capabilities expected of all employees across the Society:

- '**People we serve' centric:** (Level 3) Manage the delivery of high-quality services that provide a hand up for the people we serve.
- **Values based leadership:** (Level 4) Manage teams and areas of work to align to the Society's mission, vision, values and lay Catholic heritage.
- **Impact focus:** (Level 4) Manage the delivery of positive impact through informed decision making and efficient and effective use of resources.
- **Collaboration:** (Level 4) Manage collaboration with Conferences, directorates and teams to create opportunities, solve challenges, foster the Society's mission and implement the Strategic Plan.
- **Change leadership:** (Level 4) Manage and mobilise resources to deliver change.
- **Team performance:** (Level 3) Manage and develop individuals and teams to deliver against Society's strategic priorities.
- **Digital engagement:** (Level 4) Promote digital engagement of virtual, dispersed stakeholders to maximise efficiency and effectiveness.
- **Innovation and improvement:** (Level 3) Facilitate an improvement in existing and new services, and ways of working.
- **Financial acumen**: (Level 3) Manage the team's resources, projects and services to deliver positive outcomes within budget.

Role-specific criteria

- Tertiary qualification/s in Information Technology, Computer Science or related field.
- Relevant certifications / qualifications for example, CISSP, Security+ and other vendor related security certifications.
- Strong background in working with Industry standards: e.g. NIST or ISO 27001 is preferred
- Must be capable of providing deep knowledge support for 3 or more information security technology skill sets:
    - Access Control
    - Application Security
    - Business Continuity and Disaster Recovery Planning
    - Cryptography
    - Operations Security
    - Security Architecture and Design
    - Telecommunications and Network Security
- Good working knowledge of current IT risks and experience implementing security solutions.
- Experience implementing identity management or related technologies.
- Previous experience developing, implementing and monitoring of a strategic, comprehensive enterprise information security and IT risk management program
- Substantial private, hybrid and Azure Cloud development, implementation and operations experience.
- Substantial experience developing and implementing with Microsoft Azure, Azure AD, Windows and AD.
- Substantial experience implementing Security strategies.

Desirable criteria

- Experience working in a membership-based organisation to support and empower members and volunteers.
- Substantial experience working in a mature DevOps environment.
- Experience working on projects with digital, mobile and CRM platforms.
- Demonstrated ability to communicate with gravitas, confidence and authority in vocabulary and style appropriate to the audience.