Information Security Manager

Position Description

Directorate:	Corporate Services
Reports to:	Chief Information Officer
Reports:	**Direct**: Cyber Security Architect **Indirect**: Team Information Security Officers
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 Information Security Manager will:

- Implement cyber security strategies for the Society that enable stronger resilience to cyber security threats, ensuring compliance with appropriate security technologies, architectures, policies and compliance frameworks to protect the organisation's systems and information.
- Identify and manage risks associated with corporate infrastructure and connectivity. Develop, implement and monitor a Security Risk Mitigation program, in collaboration and consultation with the Governance Risk and Safeguarding team and appropriate stakeholders.
- Manage a Security Operations Service Provider to scan for, identify and test for security vulnerabilities and detect, analyse and respond to security events and incidents targeting network infrastructure, sensitive data, intellectual property, and employees.
- Coordinate and oversee Red Team functions such as Penetration Testing, War Gaming and Product Security Testing and Evaluation
- Supervise and oversee the review, negotiation and drafting of vendor contracts, tender documents and other legal documents and proceedings.
- Review and assess Technology controls to ensure ongoing effectiveness of policies, standards and control mechanisms by conducting audits and assessments on vendors, partners and internal teams and systems to identify security issues and gaps in governance, risk and compliance. Propose solutions to ensure business, supply chain, statutory and legislative obligations and standards are met, and the organisation is positioned to effectively respond to incidents.
- Develop, communicate, and monitor, together with Team Information Security Officers, a Disaster Recovery Plan that achieves the business continuity requirements of the organisation.
- Track and maintain all reports and actions needed to achieve compliance against security policies, regulations, and audits.
- 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 and ASD EE Cyber Security Maturity reporting
- User cyber security awareness levels
- Vendor and supply chain cyber security maturity levels

- Effective Incident and DR testing

Key working relationships

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

- Executive Directors and Directors as required.
- Technology leadership team (Corporate Services);
- Team Information Security Officers
- Key users
- 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 3) Manage teams and areas of work to align to the Society's mission, vision, values and lay Catholic heritage.
- **Impact focus:** (Level 3) Manage the delivery of positive impact through informed decision making and efficient and effective use of resources.
- **Collaboration:** (Level 3) 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 3) 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.
- Required Cyber certifications CISSP, CISM, CISA.
- Strong background in working with Industry standards: e.g. NIST (preferred) or ISO 27001
- Demonstrated experience with and knowledge of:
    - Zero Trust Architecture

  - Access Control
  - Disaster Recovery Planning
  - Security Operations

- Experience implementing and/or managing SOC or MDR vendors
- Previous experience implementing and monitoring of a comprehensive enterprise information security and IT risk management program
- Substantial private, hybrid and Azure Cloud monitoring experience, preferably with a SOC.
- Substantial experience securing Microsoft Azure, Azure AD, Windows, M362, D362 and AD environments.

Desirable criteria

- Experience working in a membership-based organisation to support and empower members and volunteers.
- Substantial experience working in an agile, scrum environment.
- Experience working on projects with digital, mobile and CRM platforms.
- Experience with Microsoft 365 Defender, Microsoft 365 Compliance Center, and Qualys