POSITION DESCRIPTION – TEAM MEMBER

Position Title	Information Security Analyst	Department	Information Technology
Location	Sydney	Direct/Indirect Reports	0
Reports to	Information Security Manager	Date Revised	May 2019
Industrial Instrument	Social Home Care and Disability Services Award		
Job Grade	Job Grade 6		

■ Position Summary

The Senior Information Security Analyst assists the Information Security Manager by planning, coordinating and performing regular security reviews/ assessments of the enterprise IT systems/ applications as well as monitoring security events/ alerts and responding to security incidents.

The Senior Information Security Analyst will also perform third-party service provider/ service assessments, follow-up on risk mitigation actions and maintain up-to-date records of third-party risks. The Senior Information Security Analyst will coordinate security assessments and IT audits performed by third-party security specialists/ auditors; review and discuss findings as well as conclude assessment reports; and coordinate and tracking the closure of vulnerabilities with internal and external stakeholders. The Senior Information Security Analyst will maintain effective operations of Information Security tools and solutions.

The Senior Information Security Analyst will assist the Information Security Manager formulate Information Security policies, standards, procedures as well as technical baselines and facilitate their enforcement/ adoption. The Senior Information Security Analyst will assist the Information Security Manager maintain up-to-date security operations registers/ records.

■ Position Responsibilities

Key Responsibilities

Strategy & Planning

- Formulate and maintain Information Security policies, standards, procedures and technical baselines
- Evaluating third-party service providers, systems and services; identify risks and provide recommendations
- Plan, coordinate and execute Information Security reviews/ assessments both internally and externally
- Perform Information Security risk assessments across the organization
- Actively contribute to the Information Security and IT strategy, architecture and roadmap
- Actively contribute to Information Security and IT governance, monitoring and reporting

Acquisition & Deployment

- Coordinate, implement and maintain Information Security Management System (ISMS)
- Evaluate, coordinate, acquire and implement Information Security tools and solutions
- Maintain up-to-date knowledge of vulnerabilities, exploit techniques, tools and solutions
- Maintain up-to-date knowledge of secure programing and secure system configuration practices

Operational Management

- Maintain up-to-date security operations registers (information assets, privileged access, remote access, risks, corrective actions, suppliers, third parties, incidents and exceptions)
- Configure, manage, maintain and operate Information Security tools and solutions (vulnerability assessment tools, security information and event management (SIEM) tools, advanced threat management tools and data/ information protection tools)
- Coordinate and execute vulnerability scans and data discovery scans and reporting
- Coordinate security assessments, compliance reviews and IT audits performed by third-party security specialists/ assessors/ auditors
- Review security assessment findings, coordinate and conclude security assessment reports, follow up on remediation action plans, maintain records and report on progress
- Follow-up, coordinate and track closure of vulnerabilities with internal and external stakeholders
- Monitor security alerts, investigate, follow-up on remedial actions with stakeholders and coordinate incident response, resolution, tracking and closure

■ Position Selection Criteria

Technical Competencies

- Good analytical and technical skills
- Five years' experience in security monitoring and IT security assessments/ reviews
- Experience in implementing, configuring and operating leading vulnerability assessment tools
- Experience in configuring and monitoring leading security information and event management (SIEM) tools
- Experience in implementing, configuring, operating and monitoring data leakage prevention (DLP) tools
- Experience in configuring and monitoring advanced threat management tools
- Good understanding of ISO27001 information security management system (ISMS) standard
- Good understating of secure IT system configurations and secure development practices
- Background in payment card industry data security standards (PCI DSS) will be considered an added advantage
- Background in IT security consulting/ auditing will be considered an added advantage

Qualifications/Licenses

- Degree qualified or significant experience in Information Security/ Cyber Security is essential
- Significant experience in monitoring and/ or performing similar scale IT security assessments is essential
- One or more information security certifications will be essential (CISSP – Certified Information Systems Security Professional, CISM – Certified Information Security Manager, CISA –Certified Information Systems Auditor, ISO27001 Lead Auditor/ Lead Implementer).
- One or more industry certifications for security assessments will be considered an added advantage (OSCP – Offensive Security Certified Professional, GPEN – GIAC Certified Penetration Tester, GWAPT – GIAC Web Application Penetration Tester, EC-Council LPT and CEH - Licensed Penetration Tester and Certified Ethical Hacker).

Behavioural Capabilities

- **Personal effectiveness | Achieve results |** Demonstrated ability to manage work and achieve the results committed to. Ability to evaluate progress and make adjustments needed to achieve goals. Accept responsibility for mistakes and learn from them.

- **Personal effectiveness | Solving problems |** Demonstrated ability to identify situations or issues, consider options and develop solutions. Ability to communicate any problems, implement solutions and monitor appropriate actions.
- **Team effectiveness | Collaborating |** Demonstrated capability to work with others to reach common goals, sharing information, supporting and building positive and constructive relationships.
- **Organisational effectiveness | Innovating and improving |** Demonstrated ability to identify and raise issues regarding ineffective work processes and take initiative to make improvements.
- **Organisational effectiveness |Managing risk |** Demonstrated ability to work within guidelines, policies and procedures. Awareness of risks involved in an individual's role and works toward minimising their impact.

■ General Conditions

All Red Cross staff and volunteers are required to:

- Adhere to the 7 fundamental principles of Red Cross:

  Humanity | Impartiality | Neutrality | Independence | Voluntary Service | Unity | Universality

- Act at all times in accordance with the Australian Red Cross Ethical Framework and Child Protection Code of Conduct
- Demonstrate skill, knowledge and behaviour to work with Aboriginal and Torres Strait Islander people in a culturally respectful way
- Comply with the Work Health and Safety management system
- Undertake a police check prior to commencement and every 5 years thereafter. Police check renewals may be required earlier than 5 years in order to comply with specific contractual or legislative requirements
- Support a child safe organisation by undertaking screening for suitability to work with children, youth and vulnerable people and to comply with relevant state/territory legislative requirements
- Assist the organisation on occasion, in times of national, state or local emergencies or major disasters