

Position Title:	Senior Security Analyst
Location:	Brisbane Head Office
Last Review Date:	May 2019
Approved By:	

Department/Team:	Financial Delegation:
> ICT	> n/a
Direct Reporting Line:	Professional Reporting Line:
> ICT Operations Manager	>

Our Vision

We will improve the health of people in remote, rural and regional Queensland.

Our Mission

We will provide excellence in, and access to, primary health care and aeromedical services across Queensland.

Our Promise

Further Corner, Finest Care.

Values

Safety and Quality > At all times, with a patient-centred focus

Mutual Care and Respect > For patients, supporters, stakeholders and each other

Commercially Astute > Agile and forward-thinking, to lead the RFDS into the future

Open and transparent > In all our dealings

Collaborative > Encouraging and empowering of each other

Proud and passionate > In all that we do

Title	Position Description - Employee	Document Id	D00200065
Parent	Human Resources Manual HRM-01	Version	14.0
Chapter	Recruitment and Selection	Modified	27/02/18

Position Purpose

The Senior Security Analyst will provide support to the ICT Operations Manager and the ICT Governance Manager in the management of the ICT Security function, ensuring delivery of ICT services and systems, and supporting a secure, sustainable ICT environment. Working closely with internal stakeholders and vendors in designing, developing and implementing user and system security controls, the role will be responsible for end-to-end security of systems, services and accounts. The Senior Security Analyst will be able to understand the requirements of the business, legal and regulatory compliance, best practice in ICT Security and clearly articulate changes required to ensure security systems continue to lift the organisation's capability.

The Senior Security Analyst will proactively investigate and respond to security incidents, identify operational security risks and provide guidance for implementing security risk mitigation activities, assist in the deployment of new security technologies, and monitor emerging security technologies, issues and directions. The role requires analysis of detected security events and information to determine the event's validity and impact, triage and remediation of security incidents and escalation where necessary, and effectively liaising with business areas and third party service providers as required, for incident response, remediation or intelligence.

The Senior Security Analyst will be responsible for managing security and access requests, increasing security awareness through communications and training, developing and implementing security controls appropriate for the business, and maintaining operational effectiveness by remaining customer focused. The Senior Security Analyst will be part of an internal ICT Team managing tickets, job priorities, liaising with third party vendors, and ensuing SLAs are met.

All employees have responsibilities for ensuring the safety of our patients and the quality of our services, these responsibilities include following procedures, modelling positive behaviours in line with our Code of Conduct, providing support, supervision and coaching to peers and junior employee team members.

RFDS Behavioural Competencies	
Analysis & Problem Solving	<ul style="list-style-type: none"> > Breaks information into component parts, patterns and relationships > Probes for further information or a greater understanding of a situation > Uses logical and rational judgement and criteria
Communication	<ul style="list-style-type: none"> > Confidently represents self and the RFDS > Maintains professionalism in verbal, written, and electronic communication within and > outside the RFDS

Title	Position Description - Employee	Document Id	D00200065
Parent	Human Resources Manual HRM-01	Version	14.0
Chapter	Recruitment and Selection	Modified	27/02/18

	<ul style="list-style-type: none"> > Adjusts style to suit the person and the scenario
Forward Thinking & Planning	<ul style="list-style-type: none"> > Anticipates relationships between current plans, tasks, situations and future events > Manages time effectively > Anticipates implications due to changed circumstances
Responsibility & Accountability	<ul style="list-style-type: none"> > Ensures expected performance outcomes are achieved > Demonstrates initiative > Is accountable for their decisions and individual outcomes
Decisiveness	<ul style="list-style-type: none"> > Prepared to make decisions > Commits to a definite course of action > Decisions and actions taken are appropriate to the situation
Productivity	<ul style="list-style-type: none"> > Works in a systematic, methodical and orderly way > Maintains quality at all times > Uses assigned resources to achieve desired objectives

Title	Position Description - Employee	Document Id	D00200065
Parent	Human Resources Manual HRM-01	Version	14.0
Chapter	Recruitment and Selection	Modified	27/02/18

Responsibilities and Measures of Success in the Role		
Key Result Areas	Responsibilities / Tasks	Key Performance Indicators
ICT Security	<ul style="list-style-type: none"> > Investigate security incidents with security vendors > Perform security risk analysis and comprehensive threat risk assessment for specific projects > Advise application managers on appropriate security controls required for compliance > Ensure patch management activities are regularly performed and kept up to date > Lead efforts in industry standards and regulatory compliance such as ISO 27001/27002, PCI, and others > Maintain a good understanding of Data Protection requirements and its implications for business areas, providing appropriate advice and practical support for current and emerging data protection requirements > Participate in the broader Information Security governance process with key information management teams > Lead and support internal/external audits, facilitate business team driven and third-party security audits/assessments > Continually review potential security risks and propose mitigation strategies > Manage day to day relationship with security vendors ensuring SLAs are met > Provide advice to the ICT Operations Manager and CIO on ICT security related issues > Develop and manage access management processes and role-based access management framework 	<ul style="list-style-type: none"> > ICT security risks are visible to executives and senior management, and being actively managed > Active programs are in place to reinforce key ICT Security risk mitigations > Breaches and incidents are reported within relevant timeframes and remedial actions taken as per policy > Respond and address any ICT security concerns of the business in an effective and efficient manner > Key risk indicators and controls are aligned to agreed security tolerances > RFDS ICT systems in general are functional and maintained to a reasonable security standard > ICT security incidents are appropriately managed and post incident reviews are conducted as required > ICT Access and Change management processes are adhered to > Third party providers are engaged and responsive within the ICT Security processes

Title	Position Description - Employee	Document Id	D00200065
Parent	Human Resources Manual HRM-01	Version	14.0
Chapter	Recruitment and Selection	Modified	27/02/18

Technology Management	<ul style="list-style-type: none"> > Ensure access management requests are assessed and performed in line with information management and security policies > Security architecture is documented and implemented in identity management systems and associated applications > Conduct market research to remain current and informed as to industry trends and emerging technologies to support best practice in security, innovation and improved stability of the ICT environment > Ensure compliance with best practice ICT security and ITIL processes > Maintain a strong understanding of current ICT systems ensuring these deliver on varying security and business needs and deliver beneficial and efficient organisational outcomes 	<ul style="list-style-type: none"> > System access requests are processed in line with agreed SLAs > Opportunities of current ICT systems and assessment of security requirements are identified, and recommendations provided to senior management for informed decisions > System security architecture, defined standards and protocols are developed and maintained > RFDS ICT environment is compliant with best practice security and ITIL processes
ICT Services and Performance	<ul style="list-style-type: none"> > Develop and maintain a prioritised work program and schedule for assigned security projects > Ensure well developed communication and change management plans exist for any upgrade or changes to the ICT security architecture > Manage assigned ICT problems, identifying root cause and developing resolution strategies > Identify ICT related risks, issues and mitigation strategies and escalate to management 	<ul style="list-style-type: none"> > ICT Team, ICT vendors and employees are kept abreast of any security matters or changes to the ICT environment and are capable of responding to those changes > ICT security incident and problem management targets are achieved > ICT risks and issues are identified and mitigated
Contributing to a High Performing Culture	<ul style="list-style-type: none"> > Understands and supports the strategic and commercial objectives of the organisation, assimilating key messages and asking clarifying questions to ensure alignment and commitment > Looks for opportunities to challenge the status quo and explore new ideas, and works with team and leader to 	<ul style="list-style-type: none"> > Demonstrated up-to-date knowledge of key messages, updates and activities across the entire organisation > Demonstrated examples identifying and participating in changes that align to organisational values and objectives

Title	Position Description - Employee	Document Id	D00200065
Parent	Human Resources Manual HRM-01	Version	14.0
Chapter	Recruitment and Selection	Modified	27/02/18

	<p>implement changes that add value and improve service delivery</p> <ul style="list-style-type: none"> > Is a supportive and cooperative team member, remaining aware of workload and activities within the team and proactively seeking opportunities to assist team and leaders where possible > Works positively with cross-functional team members, seeking to understand differing priorities and utilise strengths, and to work as an aligned and cohesive RFDS team > Takes accountability for own behaviour and performance, adopting a “no blame” approach that focuses on collaboration, learning and solutions 	<ul style="list-style-type: none"> > Leader and peer feedback reflects cooperation and support > Leader and peer feedback reflects collaboration, and that competing interests and priorities are handled respectfully and escalated appropriately > Meets role expectations and set KPIs are understood, owned and achieved
Performance and Development Review	<ul style="list-style-type: none"> > Positively participates and contributes to the RFDS' Performance and Development Review program 	<ul style="list-style-type: none"> > Completes self assessments on an annual basis or as requested by Manager / HR > Constructively and positively participates in performance discussions
Quality and Compliance	<ul style="list-style-type: none"> > Ensures a safe working environment for all employees by compliance with all relevant Occupational, Health, Safety & Welfare and Equal Employment Opportunity obligations > Contributes to business improvement/quality programs and enterprise risk management activities > Complies with RFDS policies and procedures > Ensures conduct at all times is professional, reputable and in accordance with philosophy and direction of the RFDS 	<ul style="list-style-type: none"> > Compliance with all Occupational, Health, Safety & Welfare and Equal Employment Opportunity obligations > Knowledge, understanding and compliance with RFDS policies and procedures, standard operating procedures and protocols

Title	Position Description - Employee	Document Id	D00200065
Parent	Human Resources Manual HRM-01	Version	14.0
Chapter	Recruitment and Selection	Modified	27/02/18

Working Relationships	
Internal	External
<ul style="list-style-type: none"> > All RFDS Employees and Managers > Other RFDS Sections > RFDS Board 	<ul style="list-style-type: none"> > The general public > Other primary health care organisation and service providers > Government, non-government, and community organisations > Volunteers, fund raisers and donors > All other RFDS stakeholders

Qualifications / Registrations / Memberships
<ul style="list-style-type: none"> > Formal qualifications in information, communications or technology from a recognised tertiary institution or extensive demonstrated equivalent skills and experience > ITIL V3 Foundation training and certification highly desirable > CISSP, CISM and/or CISA highly desirable

Essential skills and experience
<ul style="list-style-type: none"> > 6+ years of experience in ICT Security and/or support functions > Exceptional technical knowledge of hardware and software solutions and how it is applied to business processes > Experience in Cloud technologies, such as Microsoft Azure or AWS > Experience with Active Directory, MS Exchange Server/Exchange Online, Anti-virus and backup software and Office 365 > Change Management experience

Desirable skills and experience
<ul style="list-style-type: none"> > IT Audit/Compliance experience > Experience with ServiceNow, Office 365 applications including Teams, Skype (Online) and SharePoint (Online) operations

Title	Position Description - Employee	Document Id	D00200065
Parent	Human Resources Manual HRM-01	Version	14.0
Chapter	Recruitment and Selection	Modified	27/02/18

Additional Information

- > This role will be required to undergo a pre-employment drug and alcohol test and will continue to be subject to random drug and alcohol testing
- > This role will need the ability to travel within Queensland
- > This role will need the ability to work out of hours to respond to major incidents affecting critical systems

Title	Position Description - Employee	Document Id	D00200065
Parent	Human Resources Manual HRM-01	Version	14.0
Chapter	Recruitment and Selection	Modified	27/02/18

Sign off:

The details contained in this document are an accurate statement of the duties, responsibilities and other requirements of the position.

Wolfgang Krause
Chief Information Officer

29/05/2019

Andrew Barron
Chief Operating Officer

Date

Phoebe Burgess
Head of People & Culture

Date

As occupant of the position I,....., acknowledge, understand and agree to the statement of duties, responsibilities and other requirements as detailed in this document.

(Employee Signature)

Date

Title	Position Description - Employee	Document Id	D00200065
Parent	Human Resources Manual HRM-01	Version	14.0
Chapter	Recruitment and Selection	Modified	27/02/18