Position Description

Role Title:	**Cloud Security Engineer**
Organisation:	Mater Misericordiae Limited
Service Stream/Division:	Digital Technology and Information Division
Department/Unit:	Digital Infrastructure
Date Created/Reviewed:	July 2021
Reports To:	Product Manager – Cloud and Infrastructure Platforms
Level of Accountability:	Team Member

Role Purpose

The Cloud Security Engineer is responsible for leading the design, development and delivery of technical platform solutions for the Mater public and private cloud platforms. This role will drive cloud native technology adoption and automation practices ensuring they meet the DevSecOps requirements of our Digital Plan.

The role will work closely with leaders, architects, engineers, developers, testers, managed service providers and non-technical stakeholders, relying on the ability to articulate arguments and set the direction of solution development.

As a Lead, this role will additionally be tasked with taking on the technical leadership and direction for the organisation's Cloud Engineering, DevSecOps standards, practices, tooling and processes. A key skill will be the ability to bring people together in order to solve technical problems, direct the work of team members and deliver great results.

Behavioural Standards

This role requires the incumbent to adhere to the Mater behavioural standards including the Mater Mission, Values, Code of Conduct, Mater Credo as well as any other relevant professional and behavioural standards, translating these into everyday behaviour and actions, and holding self and others to account for these standards.

Accountabilities

Mater requires every Mater Person to understand and deliver on a series of accountabilities that are linked to the Mater strategy, described in the table overleaf. Each Mater Person is held accountable for his or own behaviour, performance and development, and for contribution to five strategic objectives: Safety, Experience, Quality, Efficiency and Financial Viability. In addition, Mater managers and leaders are accountable to different extents for clinical outcomes, service and operational outcomes, financial outcomes, compliance and risk, interprofessional leadership and management of performance and accountability.

This role is responsible for fulfilling the following accountabilities:

In this Role	
Role requirements	Is clear on the behaviour, tasks and accountabilities that are associated with the role, fulfils mandatory and professional competency requirements, contributes to own performance development planning, proactively seeks feedback and carries out individual development plan and actively contributes to their team.
As a Mater Person	
Safety	Every decision and every action taken has safety as its guiding principle.
Experience	Consistently seeks to meet or exceed each person's service expectations, each and every time through the provision of differentiated customer service.
Quality	Consistently seeks to continuously improve the quality of our service, through contributing to delivering evidence based low variability healthcare
Efficiency	Seeks opportunities to deliver services for more people within existing resources, which mean being innovative and focussed, and demonstrating strong stewardship of our finite resources.
Future Viability	Consistently seeks to improve, innovate and evolve, through looking for new trends and opportunities which will ensure Mater can meet the challenges of the future by making sensible decisions today.

Role Specific Expectations

- Designing, provisioning and maintaining Cloud environments using Infrastructure as Code automation tooling, templates, pipelines, and addressing day-to-day issues.
- Set standards for Cloud Engineering tools and techniques, including security guidelines, and the selection of appropriate DevSecOps tools and methods.
- Advise on the application of Cloud platform technologies, standards and methods and ensure compliance.
- Designing, provisioning and maintaining effective billing and monitoring solutions for all Cloud based solutions.
- Use operational data to discover opportunities to optimise Azure components for cost, processing-efficiency and reliability, plus discover tasks that can be fully automated.
- Automate processes in concert with other engineering or operational teams.
- Reporting on key metrics to management.
- Take technical responsibility for all related stages and/or iterations in a project, provide method specific technical advice and guidance to project stakeholders.
- Assign work packages, monitor performance and manage change control dynamically, to optimise productivity.
- Maintain secure configuration, apply tools, techniques and processes to identify, track, log and maintain accurate, complete and current information.
- Maintain an in-depth knowledge of specific specialisms and provide expert advice regarding Cloud Engineering and DevSecOps.
- Supervise specialist consultancies where required.
- Recommend design structures and tools for systems which meet business needs and take into account target environment, performance and security requirements of existing systems.
- Deliver technical visualisation of proposed solutions for approval by stakeholders and execution by engineers and developers.
- Translate logical designs into physical designs and produce detailed design documentation. Map work to user specification and remove errors and deviations from specifications to achieve user-friendly processes.
- Investigate and document the internal control of specified aspects of automated or partly automated processes and assess compliance with the relevant standard.
- Investigate problems in cloud related systems, processes and services. And where necessary lead or assist with the implementation of agreed remedies and preventative measures.
- Assess and analyse engineering, development, release and support practices.
- Contribute to the continual improvement of the practice of Cloud Engineering and DevSecOps.
- Be actively involved in developing and optimising processes to create efficiencies in daily operational activities.
- Participate in Change Management practices and provide recommendations for process improvements.
- Train other staff on usage of Cloud technologies and other automation related technologies.
- Assist with recommendations of training materials on new and/or existing Cloud related technologies.
- Implement, follow and support relevant policies and rules regarding Mater's legal responsibility in the areas of security, regulatory compliance, human resources.

- Acts as a champion, support and advocate for DTI initiatives across Mater including the implementation of the Digital Strategy.
- Operate within the Information and Technology operational framework (ITIL) including issue management within defined SLA's.

- This role may be required to provide support outside of core business hours.

Compliance and Risk

- Identifies, reports, responds to and rectifies workplace health and safety (WHS) concerns from within own reporting structure.
- Continuous Vulnerability Scanning (e.g. Tenable.io)
- Cloud Security solutions (e.g. MCAS)
- Experience and knowledge of Azure Sentinel workbooks
- Designing and implementing security policies and practices on Cloud environments including Azure
- Intermediate-level knowledge in one or more specific technical areas, such as development, network/cloud security, malware detection/analysis, threat intelligence, cryptography, vulnerability management, incident response, forensics, social engineering, or hacking technique

Qualifications

- A tertiary degree in area of subject matter expertise or Information Technology is highly desirable.
- Education or training in information technology and industry certifications are highly desirable.
- Postgraduate qualifications in business management, information technology, leadership, organisational change, or similar field are desirable.
- The below vendor certifications are highly regarded:
    - Microsoft Certified: Azure Administrator Associate
    - Microsoft Certified: Azure Developer Associate
    - Microsoft Certified: Security Operations Analyst Associate
    - Cyber Security related certifications: CISSP, CEH, GPEN
- ITIL Foundation is desirable.

Technical Competencies

- 2+ years of experience designing and implementing cloud solutions on Microsoft Azure cloud platform in a medium to large organisation.
- Knowledge of various cloud platforms (e.g. AWS, Google) is desirable.
- Strong knowledge of cloud security concepts and controls, encompassing IaaS, PaaS and SaaS.
- Strong knowledge of cloud networking, including NVA's, routing, network security groups, application gateway, load Balancing and private cloud connectivity.
- Experience with the following Azure services: integration, application, database and analytics.

- Experience with automation/configuration management using Azure Automation, ARM, Terraform, CloudFormation, Ansible, Puppet, Chef or an equivalent.
- Experience with CI/CD pipeline development for deploying Infrastructure as Code.
- Experience with ARM templates and JSON.
- Strong experience in scripting (e.g. PowerShell, Python).
- Understanding of firewalls is desirable.
- Knowledge of best practices and IT operations for High Availability workloads.
- A solid understanding of networking and core Internet protocols (e.g. TCP/IP, DNS, SMTP, HTTP, and distributed networks).
- Demonstrated knowledge and experience in DevSecOps.
- Knowledge of Solution Delivery Lifecycle methodologies (Waterfall & Agile) is highly desirable
- Ability to lead and mentor less senior staff and share knowledge, experience and expertise.

Capabilities

Mater's Core Capabilities	Elements	Required proficiency for Role [1]				
		Foundation (Team Member)	Proficient (Team Leader)	Skilled (Manager)	Expert (Director)	Mastery (Executive)
Building high-performance interprofessional teams: Builds high performance interprofessional teams by developing talent and building trust	Vision and direction Implementation of strategy Interprofessional practice and education Team leadership Team development Identifying and nurturing talent Building trust			✓		
Accountability: Role models respectful accountability, effectively holds self and others to account through constructive feedback and dialogue	Holding to account Feedback and dialogue Drive for results		✓			
Learning Agility: Is comfortable with complexity and ambiguity, rapidly learns and applies new skills and is successful in first time challenging situations	Comfort with ambiguity Applies learning to achieve success in challenging first-time situations Critical thinking					✓
Enacting behavioural change: Skilled at enacting sustainable behavioural change in people (through workflows, habits and clinical practice) to achieve improvements	Influencing perception Generating emotional responses (tempered by rational responses) Shaping behavioural decision making Mobilising and sustaining behaviour change		✓			

[1] **Proficiency descriptors**

- **Foundation:** demonstrates application of capabilities for performing core requirements of the role **and**
- **Proficient:** demonstrates application of capabilities to others in team **and**
- **Skilled:** developed capability in others in a proactive and structured manner **and**
- **Expert:** mobilises collective capability across teams and
- **Mastery:** is a role model within and outside the organisation and expertise as a leader in field is sought out