Job Title: **P r o g r a m M a n a g e r**			
Business Unit:	Piramal Swasthya	**Domain:**	Social Sector
Location:	PSMRI office, Hyderabad	**Big Bet:** Shared Services	**Department:** IT
Purpose of Job	Design, implement, and maintain scalable, secure, and high-performance DevOps practices on AWS infrastructure. Drive the integration of security into every phase of the DevOps lifecycle. Support automation, deployment, monitoring, and security hardening to achieve agility, reliability, and compliance.		
Key stakeholders	**External**	**Internal**	
	Cloud Service Providers, DevOps & Security Tool Vendors	Development Teams, Security Teams, QA Teams, Project Managers	
Reporting structure	**Role directly reports to**	**Positions that report into this role**	
	Sr. Manager IT	NA	
Essential Qualifications	• Any Graduate, preferably bachelor's degree in computer science or information technology. • Overall Working Experience of 6-8 Years • Minimum 4 years of experience in DevOps with AWS and security automation • AWS Certified DevOps Engineer / AWS Security Specialty (preferred)		
Preferred Key Skill /Qualifications	• Deep understanding of AWS services (EC2, S3, IAM, RDS, Lambda, CloudTrail, CloudWatch, Config, GuardDuty, VPC, EKS, CloudFormation) • Infrastructure as Code (Terraform, AWS CDK, CloudFormation) • Network security, firewall configuration, security groups, VPC subnetting • Identity & Access Management (IAM, RBAC, MFA, SSO) • Vulnerability assessment, penetration testing, patch management • CI/CD tools (Jenkins, GitHub Actions, GitLab CI/CD) • Scripting (Python, Bash, Shell) • Containerization (Docker, Kubernetes/EKS) • Security-as-Code and automated compliance tools (e.g., Checkov, TFSec, Open Policy Agent) • Secrets management (HashiCorp Vault, AWS Secrets Manager) • SAST/DAST tools (SonarQube, OWASP ZAP, Snyk, Fortify) • IAM roles, policies, encryption, KMS, and secure configurations • Centralized logging and monitoring (CloudWatch, ELK Stack, Prometheus, Grafana) • Excellent documentation, communication, and collaboration skills		

Essential Experience	• Automating security checks in CI/CD pipelines • Implementing least privilege access control and identity federation • Securing infrastructure provisioning and deployments • Conducting threat modeling and vulnerability remediation • Enforcing compliance and audit readiness (ISO, HIPAA, etc.) • Working knowledge of secure networking (VPCs, firewalls, VPNs, NACLs, etc.) • Incident response and root cause analysis for infrastructure issues • Partnering with infosec teams to roll out security best practices • Supporting development teams to adopt security-by-design
Competencies	• Strong analytical, problem-solving, and debugging skills • Security-first mindset across DevOps practices • Effective communicator and team collaborator • Continuous learning and proactive approach
Decision Making Control	• Choice of security tools and DevSecOps frameworks • Cloud architecture decisions aligned with compliance
Values	
Knowledge	• Expertise – in DevOps, AWS, and cloud security • Innovation – apply modern DevSecOps tooling and approaches
Action	• Entrepreneurship – identify and close security gaps independently • Integrity – build secure systems by design
Care	• Trusteeship – enforce cloud security to protect organizational data • Humility – engage with team members across disciplines
Impact	• Performance - high availability and secure environments • Resilience - anticipate and mitigate threats proactively

Key Roles/Responsibilities:

- Build and maintain AWS cloud environments with infrastructure as code
- Integrate security controls into CI/CD pipelines and DevOps workflows
- Automate security scans, testing, and compliance validation
- Support secure deployment of applications in containers and serverless setups
- Implement cloud-native logging, monitoring, and alerting systems
- Manage secrets, certificates, and access securely
- Work closely with development, infosec, and operations teams to enforce DevSecOps best practices
- Document all configurations, procedures, and known issues
- Conduct internal training on DevOps, secure coding and best security practices
- Respond to security incidents and participate in audits and reviews
- Ensure adherence to SLAs, compliance mandates, and performance KPIs