Job Description

Position:	**Senior Manager, Development Security Operations (DevSecOps)**
Department:	Information Technology Office
Reporting to:	Digital Executive
Location:	Head Office

I. Duties and Responsibilities

a. Leadership and Management

- Lead and manage the DevSecOps team, including platform engineers, DevOps engineers, security automation engineers.
- Define DevSecOps operating model, roles, responsibilities and ways of working across IT Teams.
- Coach and mentor teams on DevSecOps culture, automation, and secure delivery practices.
- Act as escalation point for major production incidents related to deployment, infrastructure or security controls.
- Educate and guide development and operations teams on secure coding practices and DevSecOps best practices.

b. DevSecOps Platform and Automation

- Design, implement and maintain the automation within the CI/CD pipeline for continuous deployment for each environment.
- Establish standardized DevSecOps toolchains for source control, build, testing, deployment and monitoring.
- Drive automation for environment provisioning, configuration management, and release management.
- Ensure high availability, performance, and resilience of production and non-production environments.
- Promote Infrastructure as Code (IaC) and configuration automation.
- Initialize and Enhance On-Primes and/or Cloud system architecture across testing/staging/production/DC/DR, ensuring uptime, performance and failover readiness.

c. Security and Compliance Integration

- Embedded security controls throughout the SDLC (secure coding, vulnerability scanning, penetration testing).
- Integrate security checks into CI/CD pipeline (SAST, DAST, dependency scanning).
- Ensure traceability, logging and auditability of changes and deployments.
- Align DevSecOps practice with NBC Regulation, IT Risk Management and internal security policies.
- Work closely with IT Security, Risk, and Audit teams to address findings and remediation plans.

d. Operations and Reliability

- Establish monitoring, alerting, and incident response mechanism.
- Improve system reliability through proactive performance monitoring and capacity planning.
- Lead root cause analysis (RCA) and continuous improvement initiatives for incidents.
- Support disaster recover (DR) and business continuity (BCP) testing from a DevSecOps perspective.
- Ensure smooth handover between development, operations and support team.
- Work closely with development and operations teams to ensure seamless security integration into all aspects of the software lifecycle.

e. Stakeholder and Cross-Functional Collaboration

- Collaborate with system development, infrastructure, security and business team.
- Ensure DevSevOps practice align with Enterprise Architecture standards.
- Provide regular reporting to management on system stability, security posture, and delivery performance.
- Manage DevSecOps vendors, tools, and service providers.
- Support digital transformation and modernization initiatives.
- Other tasks assigned by the line manager.

II. Qualification

- Bachelor or Master's degree in computer science or equivalent.
- At least 5 years of working experience in DevOps / DevSecOps, preferably in banking or financial services.
- Proven experience designing and operating CI/CD pipeline in enterprise environment.
- At least 3 to 5 years of leadership or managerial experience leading technical teams.
- Experience working in a regulated IT Environment with audit, risk and compliance requirements.
- Strong understanding of IT Operations, system availability, and Incident Management.
- Strong knowledge of CI/CD tools (e.g: Git, Jenkins, GitLab, etc.).
- Experience with containerization and orchestration (e.g: Docker, Kubernates).
- Knowledge of Infrastructure as Code and automation tools.
- Solid understanding of application security, vulnerability management, and secure SDLC.
- Experience with monitoring, logging, and performance tools.
- Experience of managing DevOps stack tools like Sonatype Nexus, Elastic, Grafana, Prometheus.
- Setup, configure and integrate applications and systems.
- Understanding the full apps, systems development life cycle.
- Deploys Monolithic and Microservices applications.
- System High Availability understanding using proxy or load balancer tools.
- Cloud Platforms understanding using Digital Ocean or AWS.
- Experience with Java programming is a plus.
- Proficient understanding of security data encryption and decryption.
- Proficient understanding of code versioning tools.
- High commitment and be willing to work under pressure.