About ACTED
Since 1993, as an international non-governmental organization, ACTED has been committed to immediate humanitarian relief to support those in urgent need and protect people’s dignity, while co-creating longer term opportunities for sustainable growth and fulfilling people’s potential. ACTED endeavors to respond to humanitarian crises and build resilience; promote inclusive and sustainable growth; co-construct effective governance and support the building of civil society worldwide by investing in people and their potential.
We go the last mile: ACTED’s mission is to save lives and support people in meeting their needs in hard-to-reach areas. With a team of 5,900 national staff 400 international staff, ACTED is active in 38 countries and implements more than 500 projects a year reaching over 20 million beneficiaries. More on www.acted.org

ACTED HQ
In ACTED HQ, more than 100 staff are dedicated to the operational support of projects implemented in our countries of intervention.

Key roles and responsibilities

OBJECTIVES

1) To ensure the performance, security and resilience of the ACTED cloud platform.
2) To implement industry best-practices in the fields of cloud-native and ‘infrastructure as code’ environments in line with ACTED policies.
3) To support the ACTED Data & Development team in the implementation of the core application stack.

KEY RESPONSIBILITIES

1. Management of the ACTED cloud platform (Azure)
   - Construct and maintain a catalogue of ACTED’s hosted services, including production and pre-production environments
   - Develop and document the necessary modules automating workload lifecycle and maintenance tasks
   - Propose and implement monitoring solutions suitable for the development and infrastructure teams
   - Implement a suitable mechanism for managing secrets and configurations for deployed services

2. Collaborate with the ACTED Infrastructure team to ensure the integration of the cloud platform with the existing ACTED technical infrastructure
   - Design product specifications, contractual requirements and technology stacks related to all technical architectures
   - Collaborate closely with development teams and promote a culture of resilient system design
   - Implement the ACTED Information Security Policy in all system designs
   - Update and maintain standard operating procedures
   - Perform security and maintenance updates as required
   - Implement backup policies and business continuity plans
   - Enforce a sound cloud financial management discipline (FinOps) by ensuring that cloud services costs are under control at any time
   - Proactively identify gaps in existing systems documentation and update documentation accordingly

3. Collaborate with the Data & Development team
   - Advise on the integration of CI/CD pipelines with the ACTED cloud platform
   - Facilitate the deployment of isolated feature-branch environments for internal testing
   - Provide mechanisms for debugging preprod and production environments for authorised developers
   - Assist with the development of REST APIs in the ACTED Core IMS application as required

4. Monitoring and incident management
   - Ensure constant system monitoring, raise alerts of any new vulnerabilities and propose solutions to the Infrastructure & Cyber-security Manager
   - Create, centralize and consolidate reports from the infrastructure and network of ACTED’s global sites
   - Design, update and implement dashboards to monitor systems performance
   - Assist IT helpdesk team with automation and provide level 2 support for tickets that require escalation
   - Be a key actor in the IT incident management process by being first responder during IT incidents and coordinating responses with stakeholders
   - Perform remediation actions and follow-up post-incident action plans
5. **Support change management**

- Ensure constant technological monitoring and perform active search of innovative solutions and service providers
- Contribute to change management and training of IT teams in the field
- Design training materials, tutorials & user manuals for field IT solutions and systems
- Contribute to the development a culture of IT security across all departments

### Required qualifications and technical competencies

- DevOps background and at least a BAC+5 qualification
- Strong proficiency designing and managing cloud native applications with microservices patterns (Kubernetes, Helm, Ansible, Docker…)
- Experience with commercial cloud platforms (Azure, AWS, Google, …)
- Experience with DevSecOps automation: CI/CD pipelines, secret management, monitoring
- Experience programming in Python appreciated
- Experience with Microsoft Azure PaaS appreciated (AKS, SQL, Redis, Elastic, Storage, …)
- Knowledge of cybersecurity best practice (ANSSI, CIS20, OWASP…)
- Ability to write technical and promote official documents and standards
- Rigorous, autonomous and organised, solution-oriented
- Fluency in English & French required

### Conditions

Salary defined by the ACTED salary grid depending on education level and experience
Medical and repatriation insurance, food vouchers ("tickets restaurant") when in HQ, 50% coverage of Paris transportation costs (Navigo Pass)

### How to apply

Please send your application (cover letter + resume) to jobs@acted.org **Ref: CDE/HQ**