

Vacancy announcement

Position	Country Information Systems Manager “Whole of Syria”	Starting date	ASAP
Location	Amman, Jordan (to work on our Syrian mission)	Type of contract	Fixed Term Contract
Contract duration	12 months (renewable)	Security Risk Level	Sensitive (2/4)

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 4,300 national staff 300 international staff, ACTED is active in 35 countries and implements more than 450 projects a year reaching over 11 million beneficiaries. More on www.acted.org

Country Profile

Number of projects	25
Number of areas	3
Number of national staff	610
Annual budget (EUR)	53.2M
Number of offices	7
Number of international staff	50

Position context and key challenges

In 2019, ACTED continued to deliver multisector emergency assistance to conflict affected communities, while supporting their efforts to create opportunities and solutions for recovery. ACTED provided large-scale responses to approximately 3 million people through water, hygiene and sanitation, shelter and non-food items, food security and livelihoods, and camp coordination and camp management (CCCM) interventions. In-camp, ACTED ensured access to water, sanitation and hygiene for over 364,000 people, and established itself as a key CCCM stakeholder. Out of camp, ACTED supported newly displaced households with emergency food and key non-food items to meet their basic needs. ACTED also contributed to economic recovery, by supporting livelihoods and providing assistance alongside the agricultural value chain in targeted communities. Through civil society and technical governance mechanisms, ACTED further supported the long-term restoration of services to enhance the resilience of conflict-affected communities.

Key roles and responsibilities

1. Digital Transformation project management

- 1.1. The CISM works closely with Legal Counsel and ACTED departments in-country as well as the HQ IT/IS department to identify and mitigate risks specific to the local context. S/he reviews current system applications, analyses trends in the sector, and leads the design and management of projects to enhance the Information Systems and ITC infrastructure of the country mission in close coordination with the HQ IT/IS department;
- 1.2. In line with ACTED's global Digital Transformation strategy, s/he contributes to the implementation of tools identified and designed by the HQ IT/IS department for hardware and software, and/or leads in-house information systems development, defines their scope and estimates staffing & financial requirements, defines programming standards and documentation requirements, and approves project schedules and scope changes for validation by the HQ IS Director;
- 1.3. S/he provides insight and technological innovation in the design of operational activities, budget, Kick Off Meetings (KOM), Close Out Meetings (COM) and end-of-project reporting, and acts as Information Systems and ITC focal point for project follow-up, actively participating in country-level coordination meetings by reporting on progress and risks.
- 1.4. S/he organizes regular training & refreshers about ACTED ITC/IS procedures, lessons learnt, FAQ, etc. through in-person training, remote (visioconference-based) sessions, *ad hoc* spot checks, prompt and appropriate feedback.

2. Data consolidation and archive management

- 2.1. Ensure the implementation of data consolidation tools in relation with HQ IT/IS department and after validation by the HQ IS Director;

- 2.2. Support the efficient & exhaustive circulation, filing & archiving of documentation as defined in ACTED manuals and procedures;
- 2.3. Carry out regular spot-checks on electronic and physical archiving and take preventative actions to ensure availability of 100% of the documentation;
- 2.4. Be responsible for the quality of data entry and control tags and the enforcement of file naming conventions, storage & indexation systems prior to archiving;
- 2.5. Contribute to developing and maintaining all country-specific database such as: supplier, assets, stock, etc.
- 2.6. In collaboration with others departments, contribute to define KPIs, and help them build reports with data visualisation.

3. ITC systems management

- 3.1. The CISM ensures that IS and ITC functions are adequately supported by sufficient qualified & trained staff. This includes planning and carrying out recruitment, designing and implementing an appropriate training program, developing workplans and follow-ups, and taking necessary corrective actions.
- 3.2. **Take part in the various** stages of recruitment for Capital Office-based national **IS** and ITC staff, as well as supporting the recruitment of international **IS** and ITC staff and interns.
- 3.3. Plan & conduct **IS** and ITC staff appraisals; identify **IS & ITC** staff with potential for internal mobility.
- 3.4. Carry out occasional support visits to all operational areas (**if the security situation allows**). On occasion, with prior approval of the Country Director (CD) and HQ, the CSIM may be required to undertake regional travel to other ACTED missions.
- 3.5. Support the ITC team in the design, development, and deployment of ITC systems and tools across the mission, in line with the digital transformation strategy defined by **the HQ IS department**, the country ITC Plan and donors' requirements. Ensure standard ITC systems and tools are routinely used in all operational areas and make regular recommendations for improvements to CD and the HQ IS department.
- 3.6. Support the ITC and Area Logistics team in ensuring fit-for-purpose, good value for money internet connectivity for all ACTED offices and guesthouses in all operational Areas, in line with local regulations and ACTED policies.
- 3.7. Advise on the ITC equipment and services' standards in all operational areas.
- 3.8. Ensure the ITC aspects of ACTED's logistics manual is applied in all areas
- 3.9. Contribute to improve ITC knowledge in all departments.

4. Cybersecurity Management

- 4.1. Audit and identify security bridge and risk on the ITC systems.
- 4.2. Contribute to improving traceability:
 - a. Ensure that all software and licenses are reported using the standard ACTED reporting tools (TITANIC)
 - b. Contribute to all investigation about cyber-fraud & cyber-attacks when required by Dir. Operations
- 4.3. Contribute to contingency planning in all operational Areas, particularly regarding asset follow-up and sanitisation, delivering trainings.

5. Reporting

- 5.1. Be overall accountable for the development and implementation of IS and ITC systems that facilitate efficient information transfer between operational Area, Capital, and HQ.
- 5.2. Bear overall responsibility for the IT TITANIC reports in close collaboration with CLM:
 - a. Compile information for the IT-04, IT-05, IT-06, and IT-07 and send the Country IT TITANIC to HQ on a monthly basis;
 - b. Review COM-02, monthly Internet and cell phone costs, and Area ITC reports.
 - c. Review and provide feedback on AST-05 prepared by Area Logistics;
 - d. Conduct monthly review of PRO-12.
 - e. Follow-up on corrections and requests for additional information from Area Logistics and ITC teams.
 - f. Verify 100% upload of scanned supporting documents (e.g. logbooks, stock cards, etc.) to the server.
- 5.3. Ensure that the ITC part of monthly Logistics TITANIC is complete and accurate before submission by the CLM, carefully checking the reliability & relevance of data reported from ITC teams.

Required qualifications and technical competencies

- Knowledge of relevant software development project management methodology and frameworks like Agile-Scrum (Kanban, XP, etc.), iterative and incremental development, and good team-coaching skills.
- Working knowledge of data protection and cyber-security risk mitigation strategies. Proven experience in development of multi-layered security in websites or applications.
- Experience or qualification in front-end software development processes and procedures. Knowledge or qualification in full stack development would be an advantage.

- Good understanding of current hardware and software technologies, including client-servers, network security, network protocols, particularly their application in remote and/or emergency settings, which may be demonstrated by past work experience or certifications. Experience and/or knowledge of data protection and/or e-voucher systems would be an advantage.
- Excellent communication skills including proficiency in English language.
- Ability to work independently, demonstrating creativity and good problem solving skills while following strict procedures, supporting multiple projects, priorities, and locations is essential.

Conditions

Salary defined by the ACTED salary grid; educational level, expertise, hardship, security, and performance are considered for pay bonus

Additional monthly living allowance

Free food and lodging provided at the organisation's guesthouse

Transportation costs covered, including additional return ticket + luggage allowance

Provision of medical, life, and repatriation insurance

How to Apply

Please send your application including cover letter, CV and references to jobs@acted.org under **Ref: CISM/WOS**