



## CONSULTANCY - TERMS OF REFERENCE

**UNRWA** is a United Nations agency established by the General Assembly in 1949 and is mandated to provide assistance and protection to a population of some 5 million registered Palestine refugees. Its mission is to help Palestine refugees in Jordan, Lebanon, Syria, West Bank and the Gaza Strip to achieve their full potential in human development, pending a just solution to their plight. UNRWA's services encompass education, health care, relief and social services, camp infrastructure and improvement, microfinance and emergency assistance. UNRWA is the largest UN operation in the Middle East with more than 30,000 staff. UNRWA is funded almost entirely by voluntary contributions.

### Consultant – Cyber Security Expert, (Local)

#### BACKGROUND

UNRWA has signed a Memorandum of Understanding (MoU) with United Nations International Computing Center (UNICC) that aims to enhance livelihood and human development opportunities to Palestine refugees in Gaza. By this new collaboration, UNRWA becomes a provider of Information Management, Technology services and capacity augmentation to UNICC technical team, on a cost recovery basis through IMTD/IT Service Center (ITSC) in HQ-Gaza.

United Nations International Computing Center (UNICC) is a UN agency that provides IT services to other UN agencies on a cost recovery basis.

UNRWA Information Management and Technology Department (IMTD) is seeking a **Cyber Security Expert** who will assist and support client organizations in establishing, implementing, maintaining and continually improving information security controls to ensure that information assets are adequately protected. The cyber security expert will also be responsible for providing active support with Cyber Security Governance practice at ICC and will provide services to client organizations independently or under light supervision. This is an opportunity to make a big impact and get lots of ownership. We are looking for someone who thrives in the very early stages of a project and is self-driven.

The consultant will report administratively to Head Information Technology Service Centre at Headquarter Gaza and technically to United Nations International Computing Center (UNICC).

#### DESCRIPTION OF DUTIES AND RESPONSIBILITIES

Under the direct supervision of Lead, Cyber security governance and in close collaboration with the Information Security Services team members the consultant will be required to:

- Develop and enhance an information security management framework based on the ISO 27000 standards;
- Develop, maintain and publish up-to-date information security policies, standards and guidelines. Oversee the approval, training, and dissemination of security policies and practices;
- Create, communicate and implement the process for risk management, including the assessment and treatment of identified risks. Work directly with business units and stakeholders throughout the organization on identifying acceptable levels of residual risk. Report and oversee treatment efforts;
- Build regular reporting/dashboards on the current status of the cyber security programme to senior management and business units as part of a strategic enterprise risk management programme;
- Help raise cyber security and risk management awareness for all employees, contractors and approved system users;
- Provide active support during security incidents and events that affect organizational assets, including intellectual property, sensitive data and the organization's reputation;
- Provide direction, support and in-house consulting in effective disaster recovery policies and standards. Coordinate the development of implementation plans and procedures to ensure that business-critical services are recovered in case of a security event;
- Provide strategic risk guidance for IT projects, including the evaluation and recommendation of technical controls;
- Ensure that security programs are in compliance with relevant rules, regulations, policies and standards to minimize or eliminate risks and audit findings;

- Monitor the external threat environment for emerging threats, and advise relevant stakeholders on the appropriate courses of action;
- Perform technical security assessments and develop strategies for remediating vulnerabilities and risks identified;
- Work closely with other members of ICC's cyber security team to develop and deliver new and existing cyber security services;
- Provide other ad hoc support either within CPI or other units as required – this includes the participation in special projects or support to service delivery for short period of time on a part-time or full-time basis upon request from the senior management.

#### **MINIMUM QUALIFICATIONS AND EXPERIENCE**

- A university degree from an accredited educational institution in Computer Science, Information Technology, or related discipline;
- Minimum of five years of experience in information security, risk management, or IT-Security or security incident response or security testing related jobs with increasing levels of responsibility;
- Experience in developing information security policies and procedures, as well as successfully executing programs in a dynamic environment;
- Excellent knowledge of information security technologies;
- Professional security management certification, such as a Certified Information Systems Security Professional (CISSP), Certified Information Security Manager (CISM), Cloud Security Professional (CCSP), Iso27001 lead implementer/auditor, or other similar credentials. .
- Fluency in spoken and written English.

#### **COMPETENCIES**

- Ability to understand technical and business aspects of IT risk, and to communicate those risks to management, business and technical units so that the organization can make informed decisions regarding appropriate levels of information security control;
- Strong analytical and problem-solving skills;
- Ability to work well in a demanding, dynamic environment. Ability to act calmly and competently in high-pressure, high-stress situations;
- High level of personal integrity, as well as the ability to professionally handle confidential matters, and show an appropriate level of judgment and maturity;
- High degree of initiative, dependability and ability to work with little supervision.

#### **DESIRABLE QUALIFICATIONS**

- Experience in achieving and maintaining ISO 27001 certification;
- Three years of experience working in security consulting engagements;
- Project management skills and ability to manage multiple projects under strict timelines;
- Knowledge of common information security management frameworks, such as ISO/IEC 27001, ITIL, COBIT, etc.

#### **CONDITIONS OF SERVICE**

- The duration of the consultancy is 6 to 11 months, extendable according to performance and availability of funds.
- Remuneration for this consultancy will depend on the qualifications and relevant experience as follows:
  - Cluster A: \$1,600.
  - Cluster B: \$1,800.
- The incumbent can be in any of UNRWA fields of operations (Gaza, Jordan, Lebanon, Syria, or West Bank).

#### **APPLICATION PROCESS**

Applicants should submit a cover letter and CV or UN Personal History Form demonstrating clearly the knowledge and experience required to meet the consultancy requirements via [consultancy@unrwa.org](mailto:consultancy@unrwa.org) indicating the title of this consultancy “**Cyber Security Expert**” in the subject line of the message and field (area)/country of the candidate. The deadline for the submission of applications is **31 January 2021**.

*UNRWA is an equal opportunity employer and welcomes applications from both women and men. UNRWA encourages applications from qualified women. Only those applicants shortlisted for interview will be contacted. UNRWA is a non-smoking environment.*

12/01/2021