Annex B

TERMS OF REFERENCE FOR SERVICE CONTRACTING

Assignment	Provide Security Access Control System for UNICEF Jordan Country office (JCO) building
Location	UNICEF JCO Premises
Duration	6 weeks
Reporting to	Country Office - Security Officer

1. JUSTIFICATION/BACKGROUND

Current access control system been installed since last three years, originally it was old technology had limited functions, not developable to meet UNICEF JCO needs and COVID-19 requirements.

UNICEF JCO has access control system to prevent and delay and unexpected violation to the premises, by implementing different security layers. Due to the location of UNICEF JCO premises at the centre of Shmaisani commercial area, the likelihood of any violation of the premises is medium, therefore we must minimize the likelihood and impact.

The current access control system is outdated, the maintenance became costly of the current system, there is no possibility of any update or develop.

We need to install new access control system with developed features that meet the prevention and delay of any violation, implement the security layers, cover all week points at the premises. This system will be able to integrate the CCTV system with access control system if requested in future, ability to develop the system based on any future required update, easy end user, availability of spare parts and maintenance in short time, no gabs or delay for maintenance. Specialised and experts for maintenance under supervision of the main manufacture.

2. OBJECTIVE AND TARGETS

The objective of this TOR is to install security access control system replacing the existing one at the new rented office building for UNICEF JCO at Al-Shmeisani area.
The building is located in a commercial area and the current access control system is not efficient, outdated not developable, therefore, we are planning to replace it with advanced system to enhance our security layers and minimize security guard's intervention and avoid hand touch or finger print.

3. SCOPE OF THE WORK (WORK ASSIGNMENT)

Install new access control system with developed features that meet the prevention and delay of any violation, control the access to the premises
Implement the security layers,
Cover all week points at the premises.
Possibility of integration between CCTV system with access control system if requested in future.
Ability to develop the system based on any future requirements or update,
Easy to be use the software for end user,
Availability of spare parts and maintenance in short time, no gabs or delay for maintenance.
Specialized and experts' staff for maintenance under supervision of the main manufacture.
Installation
Test the system after installation
Training
Provide advisory after assessment of the premises for the best interest for UNICEF JCO

4. MINIMUM REQUIREMENTS

The below are minimum requirements and bidders are expected to physically assess the office building and premises and propose suitable and appropriate system.

General Features:

- The Access Control System shall be a multi-tasking and multi-users-based head end running on a distributed TCP/IP, Wi-Fi network.
- The Access Control System shall comply to the strict regulation and adapting state-of-the-art security technologies, the highest level of reliability, and integrate to networking infrastructures such as the Intranet, Internet, LAN/WAN
- Card reader + PIN and face recognition access including duress access support, and dual cardholder authentication.
- RFID (Radio-frequency identification) distance recognize the access.
- Control outputs to manage building facilities.

- Maintain system integrity with scheduled or manual tests.
- Multiple language support.
- Integrated rear tamper.
- Fully Configurable Mimic Panel reflecting the status of up to 8 inputs, outputs.
- Upgrade software in situ to keep the system up to date with latest technology developments.
- Environmentally friendly - RoHS compliant and designed for minimal power consumption.
- Support for custom site encryption keys.
- Possibility of upgrade the system without need to change card readers, software.
- The system shall be provided to control access into designated security-controlled doors only by personnel with a valid access card or Identification PIN and within valid time schedule. All access cards shall be authenticated against the central and/or local database before granting access.
- All door access activities shall be logged into the central database.
- Any unauthorized attempt or invalid card used shall be reported to the ACCESS CONTROL SYSTEM, including door held and forced opened alarm as priority alarm transaction.
- Access Control System shall continue to operate for at least 2 hours in the event of main AC power failure. The specifier shall take in consideration the traffic loads and power consumption at each point of installation when determining the size of the Uninterrupted Power Supply (UPS) as backup power. Provision of the UPS shall be under the scope of this sub-contract.
- Upon completion of the installation provide complete training with documentations on the configuration, operation and maintenance of the systems to the required operators assigned by the owner. At least two (2) training sessions covering system operations shall be planned and provided to operators and two (2) sessions covering system administration and management for system administrators.
- The Access Control System shall be of open-architecture, PC-based system based on Windows Operating Systems, such as Windows Server 2008 (R2) and Windows 10.
- Automatic number-plate recognition system to be part of the access control system
- Possibility of integration between CCTV system and access control system

Monitoring and Control

- Lockdown areas in response to a threat or emergency.
- Confirm and control the identity of a person passing through a nominated door via visual comparison of a cardholder image.

- View cardholders currently located within selected areas.
- Integrate intranet, web or network-based alarm response instructions, or other relevant information directly to Command Centre's command and control interface via in-built browser capability.
- Control site access to ensure a free state is only enabled when a registered cardholder is present.
- Emergency switch to disable the system in case of emergency.

Configuration and Operation

- Site hardware and system components, including access, intruder alarm and perimeter security fencing
- Schedules to automate access and alarm state changes. Doors may be configured as requiring card only, card plus PIN, dual access (two unique cards), free access etc
- Entry and exit delays for intruder alarm zones
- Individually programmed responses for a cardholder or all members of an access group
- System division and assigned privileges to manage operators.
- Offline controller capability, system integrity is maintained even during loss of connection with primary servers.

Cardholder Management

- Import cardholder data, photos and access rights from third party systems via flexible XML interfaces or the simple data mapping interface provided by the Enterprise Data Import module
- Assign access rights based on the type of day, time of day, area being accessed, validity of the cardholder token, and the competencies (training, licenses, inductions or medical clearances) the cardholder possesses. Access changes are immediately and automatically downloaded to the controllers
- Manage cardholder details, view recent cardholder events from the user interface, and track card replacement history.
- Perform bulk updates of cardholder information, such as a change in department
- Design card layouts, and print and encode photo ID cards (in case we want to merge ID card with access card in one card only)
- Tailor screen layouts for the cardholder management team
- Find cardholders in the system via access card presentation, text entry or multi-statement search criteria.
- Operates with accrementition and card

Reporting

- Retrieve and report on a variety of stored information including events, cardholders and their access, cardholders and their location, site items details or exception reporting.
- Possibility to tailor our own reports and customize its up on our needs.
- View additional reports, including evacuation (also visitor data when used with visitor management functionality), access, time, and contextual reporting
- Access reports easily through a ‘find reports’ viewer or ‘favorites’ list within an application tab
- Configure cardholder reports including page layout, file output type (.doc, .xls, .pdf, or .csv) filters within the report, and more.
- Perform expanded report filter operations using parameters such as competency status, card type, cardholders last entered zone.

Visitor Management

- Sites to share host, visit and visitor configuration so that visitors arriving on-site can be managed from either a reception workstation or a kiosk
- Automatic removal of access on visit completion or when a visitor badges their card at an off-site reader
- Customizable sign-in process to allow greater flexibility in the visitor experience
- Full communication with visitor management reception, pre-registration or kiosk clients via network services over TCP/IP
- Quick identification of preregistered visitors via barcodes
- Remote, single-click client deployment and automatic client updates reducing installer time as they no longer need to visit each workstation
- A comprehensive audit trial of all visitor management events, including receptionist actions, visitor pre-registration, escort, host and visitor actions are securely maintained at the Command Centre server.

Notifications

- Event notifications via SMS or Email
- Alarm Acknowledgement via Return Message
- Scheduled event notification filters for targeted notification
- Scheduled email generated for select reports
- Expiry notifications of cards or competencies.

Command Centre Mobile App

- Manage alarms and perform common overrides away from the control room

- Challenge cardholders with the Spot Check feature, to tell at a glance if a person is authorized to be in a location, including the ability to record the reason for a fail, the location detail, and to disable the card, preventing further use.
- Manage temporary entry/exit points with the Mobile Access feature, allowing secure access control anywhere on site
- Response to open door requests from anywhere on site
- Remote monitoring the status of Access Zones, Alarm Zones, Fence Zones and Doors
- Access of relevant incident details remotely and the ability to add notes regarding an alert for control room oversight
- Trigger pre-configured macros
- Secure operation utilizing latest network security standards
- Lockdown individual zones directly from the phone
- Report visitors and staff availability within the premises.
- Integration with third party DVR/NVR systems
- Possibility to control the access (deny or permission) from control room or mobile device.

5. EXPECTED DELIVERABLES

Bidders will have the opportunity to visit the premises and assess requirements

N	Expected deliverable:	Timeframe
1.	An inception proposal with detailed implementation /action plan for the system.	1st week from signing the contract
2.	Revision of the relevant software and devices provided and future upgrade the system.	2nd week from signing the contract
3.	Deliver the system unit with software and card readers and install it.	3rd – 4th week from signing the contract
4.	Run the system as testing functionality.	5th week from signing the contract
5.	Testing the system and start issuing new access control cards, intensive training for security team with full administration and operational control.	5th week from signing the contract
6.	Ensure availability of solving troubleshooting and system faults, speed respond up on call from UNICEF.	6th week from signing the contract
7.	Submit a final report on execution of the work providing warrantee on the software and devices (card readers) upgrading plan. Service providers should provide the warranty of new equipment and the maintenance plan after the expiry of the warranty period.	6thweeks from signing the contract

5. DELIVERY DATES AND DETAILS ON HOW THE WORK MUST BE DELIVERED

- UNICEF will have a full oversight on the implementation of the work.

- Regular meetings with the supplier, Security section will be convened to review progress and encountered challenges.

6. OFFICIAL TRAVEL INVOLVED

Not applicable.

7. DESIRED QUALIFICATIONS, SPECIALIZED KNOWLEDGE OR EXPERIENCE

1. Legally registered company, with minimum two years of experience in the same field, at least three or more executed projects with the same level for reputed companies, entities or organizations, legal representative from the manufacturer of the product and system unit, Able to provide technical support 24/7, Customer service orientation.

Reference of sample work is required.

8. PERFORMANCE INDICATORS FOR EVALUATION OF RESULTS

- Timely and quality submission of deliverables.
- The contractor's fee shall be inclusive of all office administrative costs

It is expected that this access control system will be conducted from 1st October 2020. The contract would cover the entire duration of the scope of work. Proposed and estimated timeframe for deliverables is listed under each deliverable in the Section 1. The company should propose a timeline to submit the deliverables considering necessary and adequate time (at least two weeks) to be allocated for review and quality assurance processes of the deliverables by UNICEF.

9. Payment Terms

Payment will be made only upon UNICEF's acceptance of the work performed. The terms of payment are Net 30 days, after receipt of invoice and acceptance of work. Payment will be affected by bank transfer in the currency of billing.

Payment is contingent on approval by the CSFA Security Section and will be made in four installments as follows:
-10% of the total upon submission of approved inception software and devices.
-40% of the total upon Installation and testing software and devices.
-40% of the total upon the finalization, testing, training ensure system is functioning as planned, subject to security section approval.
-10% of the total Warranty will be kept for after sales services will be paid after three months' probation period.

10. Contract Management

The contractor will regularly report to UNICEF Country Security Officer. UNICEF Security management team (both Regional office and Country office) are responsible for managing the contract.

11. FREQUENCY OF PERFORMANCE REVIEWS

Overall performance at the end of the contract will be evaluated against the following criteria: customer service, responsiveness, technical competence, responsibility, initiative, communication, and quality of service and products delivered.

12. CALL FOR PROPOSALS

A two-stage procedure shall be utilized in assessing the proposals, with assessment of the technical proposal being completed prior to any price proposal being compared. Applications shall therefore contain the following required documentation:

1. **Technical Proposal:**
   Applicants shall prepare a proposal as an overall response to ToR ensuring that the purpose, objectives, and deliverables of this task are addressed. The Technical Proposal shall also include but not limited to:
   - Updated company profile,
   - Detailed implementation /action plan
   - Proposed system full description with data sheet
   - Legal registration, business license
   - Official certificate of legal representation from the manufacturer
   - Human resources profile in provision of maintenance, troubleshooting, after sales service…etc. including CVs of technical team
   - Provision of the warranty for new equipment and the maintenance plan after the expiry of the warranty period.
   - List of executed projects with project total value and detailed description, to be part of the evaluation,
   - Electronic copies/links of one or two most recent and relevant projects executed by the proposed company. Along with a recommendation letter.
2. **Financial Proposal:**
   Financial Offer detailing all activity expenses and logistics should be submitted under this section.

   Offer with cost breakdown:
   - System Unit, Software, Card readers

- Installation cost
- Preventive maintenance
- Maintenance after the expiry of the warranty period.

The Financial Proposal shall be submitted in a separate file, clearly named Financial Proposal. No financial information should be contained in the Technical Proposal.

13. UNICEF RECOURSE IN CASE OF UNSATISFACTORY PERFORMANCE

In case of unsatisfactory performance, the payment will be withholding until quality deliverables are submitted. If the firm is unable to complete the assignment, the contract will be terminated. In the meantime, UNICEF will initiate another selection in order to identify appropriate candidate, any additional cost will be charged to the company with unsatisfactory performance.

14. INDICATION THAT THE CONSULTANTS/INDIVIDUAL CONTRACTOR HAS RECEIVED A COPY OF THIS DOCUMENT OR, ALTERNATIVELY, AN EXPERT OF RELEVANT PROVISIONS INCLUDING THOSE CONCERNING LEGAL STATUS, OBLIGATIONS AND TITLE RIGHTS.

Not applicable

15. REQUEST FOR PROPOSAL EVALUATION AND WEIGHTING CRITERIA

Submitted proposals will be assessed using Cumulative Analysis Method. All requests for proposal will be weighed according to the technical (70%) and financial considerations (30%). Financial proposals will be opened only for those applications that attained **49 points** or above on the technical part. Below are the criteria and points for technical and financial proposals.

Section A: Technical proposals

1) Overall Response (**10** points)

- General adherence to Terms of Reference and tender requirements. Clear response towards the requirements of the TOR and any alternative suggestions based on Contractor's experience in other similar assignments;(5)
- Elaborate and articulate understanding of scope, objectives and overall work. (2.5)
- Completeness of response (2.5)

2) Proposed methodology and approach (**30** points)

- Deliverables are addressed as per ToR (5)
- Proposed approach/methodology and management control system respond to the scope of work. (5)
- Proposed Implementation Plan, i.e. how the bidder will undertake each task, and maintenance of project schedules demonstrates timelines will be met (5)
- Process and procedures for ethical review are elaborated and integrated into the process (5)
- Alternative proposals are made on methodology, implementation plan and timeframe as per the sound understanding of the scope of work and with reasonable justifications (5)

- Critical factors and constraints from the Contractor's perspective, which may impact the success and timely completion of the assignment/project. (5)

3) Technical capacity (**30** points)

- Company have previously conducted similar work with evidenced range and depth of experience with similar work. (5)
- Human resources profile in provision of maintenance, troubleshooting, after sales service…etc. including CVs of technical team (5)
- Proposed Software and devices with ability of future upgrade and expansion (5)
- Provision after sales service proposal and warranty for new equipment and the maintenance plan after the expiry of the warranty period. (5)
- System meets with UNICEF requirements and ability to provide additional alternatives and progressive ideas and proposals (5)
- Two Samples of previous relevant work undertaken successfully by the contractor. (2.5)
- Three separate work-related references. (2.5)

Technical score: 70 % of 70 points = 49 points

Section B: Financial Offer

A separate Financial Offer detailing all activity expenses and logistics should be submitted under this section. The financial offer (this section) should be submitted on a separate page from the Technical Capability and Schedule information.

The Technical section of the proposal should be submitted in English language. All other sections should be annexed.

16. CONDITIONS

- The contractor will work on his/her and use its own office resources and materials in the execution of this assignment.
- The contractor's fee shall be inclusive of all office administrative costs

Enquiries:

ENQUIRIES: Please direct any enquiries to the contact details indicated on the tender document

Proposals with all supporting documents should be addressed to:

UNICEF JCO Bids
jordanbids@unicef.org