

TERMS OF REFERENCE (TOR) FOR Access Control System

This TOR aims to install security access control at the UNICEF premises in Myanmar (Yangon Office)

1. Background:

Install a new access control system with developed features that prevent and delay any violation and control access to the premises. Implement the security layers, covering all weak points at the premises and possible integration between the Fire Alarm and access control systems.

-Ability to develop the system based on any future requirements or updates. Easy-to-use software for end users.

-Availability of spare parts and maintenance quickly, with no gaps or delays.

-Specialized and expert maintenance staff under the leading manufacturer's supervision. Installation tests the system after installation and training.

2. Objectives of the project:

Install security access control at the UNICEF premises in Myanmar Yangon.

3. Geographic Area:

Myanmar; within UNICEF's office in Yangon

4. Duration:

2 months

5. Supervisor:

Zar Li Maw (Administrative Specialist), Samah Al Maalouf (ICT/T4D Specialist)

6. Scope of Work:1) Initial Site Assessment

- Conduct a thorough inspection of the existing Access control system to evaluate its current condition.
- Identify areas where the Access control system is inadequate.
- Measure and document the current premises.

2) Detailed Recommendations

- Prepare detailed recommendations for the site assessment.
- Provide recommendations for necessary systems and accessories
- Suggest specific materials to be used.

3) Design and Engineering Services

- Develop a design plan for the new or upgraded system.
- Ensure that the design complies with relevant safety standards and best practices.
- Submit the design and BOQ for approval by UNICEF for installation works.

4) Testing and Verification

- Test the new access control system to verify its functionality. Provide a report on the testing results, including any necessary adjustments.

5) Post-Implementation Support

- Offer a warranty period during which any issues with the grounding system will be addressed at no additional cost.
- Provide ongoing support and maintenance as needed.

7. Service Level Agreement (SLA) Requirements for Access Control System Provider

The selected provider must commit to the following SLA terms for Access Control System service:

1. Service Availability

- **Uptime:** Guarantee a minimum of 99.9% uptime per month.

2. Incident Response and Resolution

- **Critical Incidents:** Response within 4 hours; resolution within 8 hours.
- **Major Incidents:** Response within 8 hours; resolution within 12 hours.
- **Minor Incidents:** Response within one day; resolution within two days hours.

3. If the service uptime falls below the guaranteed 99.9% per month, the provider will be subject to a penalty of 2% of the monthly service fee for every 0.1% decrease in uptime, up to a maximum of 10% of the total monthly fee.

7. Hardware and Software requirements

3.1 Access Control Hardware

3.1.1 Access Control Panels/Controllers

- **Type:** IP-based controllers with PoE (Power over Ethernet) support.
- **Capacity:** Each controller should manage at least two doors and be expandable.
- **Communication:** TCP/IP communication with the server or management software.
- **Power Supply:** 12V DC with battery backup support for at least 8 hours of operation during power outages.
- **Memory:** Non-volatile memory to store user data and access logs locally in case of network failure.

3.1.2 Access Readers

- **Type:** Multi-technology readers supporting:
 - **Proximity Card (RFID):** 13.56 MHz contactless smart card technology (e.g., MIFARE).
 - **PIN Pad:** Numeric keypad for code-based entry.
 - **Biometric:** Fingerprint scanner or facial recognition capability.
- **Operating Temperature:** -10°C to +50°C for indoor and outdoor use.
- **Housing:** Weatherproof and vandal-resistant housing (IP65 rated) for outdoor installations.
- **Response Time:** Less than 1 second for card and PIN authentication and less than 2 seconds for biometric authentication.

3.1.3 Electric Locks

- **Type:** Electromagnetic locks (maglocks) or electric strike locks.
- **Holding Force:** Minimum 600 lbs. (for maglocks).
- **Power Supply:** 12V DC or 24V DC.
- **Fail-Safe/Fail-Secure Options:** Select according to safety requirements (e.g., fail-safe for fire exits).

3.1.4. Door Position Sensors

- **Type:** Magnetic reed switches.
- **Mounting:** Surface or flush mounting options.
- **Functionality:** Detect and report door status (open/closed) to the access control system.

3.1.5. Exit Devices

- **Type:** Request-to-Exit (RTE) buttons or sensors.
- **Sensor Type:** Infrared or touchless for hands-free operation.
- **Mounting:** Surface mount near the door exit.

3.1.6. Emergency Override

- **Manual Override:** Mechanical key override or emergency release button to unlock doors in case of system failure.
- **Fire Alarm Integration:** The system should automatically unlock doors upon receiving a signal from the fire alarm system.

3.2. Software Specifications

3.2.1 Management Software

- **Platform:** Web-based interface accessible via browsers or dedicated applications for Windows, iOS, and Android.
- **User Interface:** Intuitive and user-friendly GUI for easy navigation.
- **User Management:** Ability to add, delete, or modify user profiles, access levels, and schedules. 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.
- **Access Levels:** Configurable access levels based on roles, time schedules, and building zones. 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
- **Event Logs:** Automatic logging of all access events, real-time monitoring and historical data retention.
- **Reporting:** Generate customizable reports on access activity, user attendance, and system status. 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. View additional reports, including evacuation (also visitor data when used with visitor management functionality), access, time,

and contextual reporting. Configure cardholder reports including page layout, file output type (.doc, .xls, .pdf, or .csv) filters within the report, and more.

- **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 of the status of Access Zones, Alarm Zones, Fence Zones and Doors
- Access to relevant incident details remotely and the ability to add notes regarding an alert for control room oversight
- Trigger pre-configured macros
- Secure operation utilizing the latest network security standards
- Lockdown individual zones directly from the phone
- Report visitors and staff availability within the premises.
- Possibility to control the access (deny or permission) from the control room or mobile device.

3.2.2 Security Features

- **Data Encryption:** All communications between controllers, readers, and management software are encrypted end-to-end (AES-256).
- **User Authentication:** Multi-factor authentication (MFA) for accessing management software.
- **Backup:** Automated data backup with options for local and cloud storage.

3.3. Integration Capabilities

- **Alarm System Integration:** Interface with existing alarm systems to trigger alarms based on unauthorized access attempts.
- **Fire Alarm Integration:** Automatic door release upon fire alarm activation.

- **API Support:** Open API to integrate third-party systems (e.g., HR software, visitor management systems).

4. Installation Requirements

4.1. Cabling

- **Type:** Category 5e Ethernet cables for communication, and 18/2 AWG shielded cable for power.
- **Cable Management:** Proper cable management with conduits and labeling.
- **Compliance:** All cabling must comply with industry standards (e.g., ANSI/TIA-568) and local regulations.

4.2. Mounting and Enclosures

- **Readers:** Mount at an appropriate height (approximately 48 inches from the ground).
- **Controllers:** Install in secure, climate-controlled locations within each building.
- **Lock Enclosures:** Use weatherproof enclosures for outdoor locks.

4.3. Power Supply and Backup

- **Primary Power:** 12V DC or 24V DC power supply units for each access control device.

5. Testing and Commissioning

5.1. System Testing

- **Functional Testing:** Verify the operation of all components, including readers, locks, sensors, and software.
- **Failover Testing:** Simulate power loss and network failure to ensure the system's backup functionality.
- **Integration Testing:** Ensure proper integration with CCTV, fire alarms, and other connected systems.

5.2. User Acceptance Testing (UAT)

- **Client Verification:** Before the final handover, allow the client to test the system to ensure it meets all specified requirements.
- **Documentation:** Provide detailed test reports and a checklist of all tested components.

6. Training and Documentation

- **Training:** Conduct comprehensive training sessions for system administrators and end-users.
- **Documentation:** Supply complete user manuals, installation guides, and maintenance instructions.

7. Maintenance and Support

7.1. Warranty

- **Coverage:** A minimum 1-year warranty on all hardware and software components. This includes free-of-charge regular maintenance, software updates and troubleshooting during the warranty period.
- **Service Level Agreement (SLA):** Define response times for technical support, repair, and maintenance services.

7.2. Maintenance Services

- **Preventive Maintenance:** Regular system checks and updates as per the maintenance schedule.
- **Support:** 24/7 remote and on-site support services.

8. Description of assignment, Timeline, Payment Schedule:

Tasks	End Product/deliverables	Timeline/Payment
An inception proposal with a detailed implementation /action plan for the system	Assessment proposal	One week; 30%
Installation of the relevant software and devices provided and future system upgrades. Deliver the system unit with software and card readers and install it. Run the system as testing functionality.	Hardware and software installation	One week
Testing the system, issuing new access control cards, and intensive training for the security team with complete administration and operational control.	Implement and testing	One week
Submit a final report on the execution of the work, providing a warranty on the software and device (card readers) upgrading plan.	Report handover	Two days; 70% upon the a final report

9. Qualification and specialized knowledge/experience required for the assignment:

Work experience: Proven experience in the set-up of Access control system services.

Proven Experience in Access Control Services: At least two years of experience in the design, implementation, and management of Access Control systems, preferably for large organizations or international entities.

Technical Expertise: Demonstrated expertise in telecommunications technologies and network security, including experience with secure data management practices.

Compliance with Data Protection Regulations: Comprehensive understanding of data protection laws and regulations, such as GDPR or equivalent, and experience implementing solutions that ensure compliance with these standards.

Client References: At least three references from past clients for similar projects, preferably within the humanitarian or non-profit sector.

Staffing and Support Capabilities: A dedicated team of certified professionals with the skills to manage the setup, ongoing maintenance, support, and troubleshooting of the Access Control system.

Local Presence and Understanding of Context: Preferably, a local presence in Myanmar or experience working in similar contexts to understand local telecommunications infrastructure and regulatory environment.

10. Proposal Evaluation Process and Criteria

Interested bidders are invited to visit the site (UNICEF Office in Yangon) before making an offer.

The evaluation will be carried out in two phases: technical evaluation (maximum 70 points) and financial evaluation (maximum 30 points).

The technical evaluation will evaluate each technical proposal for compliance with the technical requirements stated in this ToR according to the technical evaluation criteria stipulated in Annex 1 below. Proposals that are considered technically non-compliant or non-responsive will not be given further consideration.

Next, the financial evaluation will evaluate each financial proposal from technically qualified institutions. The maximum point (30) will be allotted to the lowest-priced proposal. All other financial proposals will receive points in inverse proportion to the lowest financial proposal, determined by the following formula:

Score of financial proposal X =

Max. score for financial proposal (30) * Price of lowest-priced proposal / Price of financial proposal X

The award recommendation will be based on a cumulative analysis of technical and financial scores.

11. Nature of Penalty Clause to be stipulated in the contract:

UNICEF Myanmar reserves the right to only pay the Contractor or withhold part of the payable amount if one or more requirements established for this assignment are met or the deadline set for accomplishing the tasks is missed.

Annex 1: Technical Evaluation Criteria

Item	Technical Evaluation Criteria	Max. Points Obtainable
1. Overall Response	Evaluate the proposer's understanding of the assignment and alignment of the proposal with the Terms of Reference (ToR).	30
1.1	Completeness of response: Clarity, comprehensiveness, and coherence of the proposal.	10
1.2	Understanding of UNICEF's needs: Demonstrates a deep understanding of the project's objectives, scope, and deliverables, including specific needs related to the Access Control services.	10
1.3	Alignment with ToR: The proposal aligns well with the requirements and deliverables specified in the ToR, particularly regarding data protection, access control, and monitoring.	10
2. Company and Key Personnel	Assesses the proposer's experience, capacity, and expertise to perform the tasks required.	30
2.1	Organizational Experience: Demonstrated experience in setting up and managing Access control systems, especially for international organizations or NGOs, with at least five years of relevant experience.	10
2.2	Relevant Projects: Quality and relevance of samples from at least three similar Access control systems completed in the last five years, with a focus on data security and user training.	10
2.3	Key Personnel Qualifications: Relevant experience and certifications of the proposed team members, including technical expertise in Access control systems and network security.	5
2.4	Client References: Positive references from at least three previous clients, preferably in the humanitarian or non-profit sector, demonstrating successful project delivery.	5
3. Proposed Methodology and Approach	Evaluate the proposed work plan, implementation strategy, and technical approach to achieve the objectives.	40
3.1	Work Plan: Detailed work plan with a timeline that reflects an understanding of the project's complexity, including specific milestones for each phase (e.g., setup, testing, training).	5
3.2	Data Protection and Security Measures: Robust strategies for data encryption, secure access controls, and compliance with data protection regulations (e.g., GDPR).	20
3.3	Monitoring and Evaluation: Proposed methods for continuous performance monitoring, regular maintenance requirements, quality assurance, and regular reporting to UNICEF on service levels and usage statistics.	5
3.4	Training Plan: Comprehensive plan for training end users and system administrators, including initial training sessions, training materials, and ongoing support.	5
3.5	Disaster Recovery and Backup: Detailed plan for disaster recovery, including Recovery Time Objective (RTO), Recovery Point Objective (RPO), and redundancy measures.	5
Total Technical Scores		100
Minimum Technical Score Required	The minimum score required to qualify for further financial evaluation	70