CALL FOR PROPOSALS
by <u>Nonviolent Peaceforce</u> as the **Client**
related to:

The development, implementation, and maintenance of Nonviolent Peaceforce's centralised Information and Communication Technology (ICT) system

- **Requested services: The development, implementation, and maintenance of Nonviolent Peaceforce's centralised ICT system**
- **Contracting organisation: Nonviolent Peaceforce**
- **Deadline for submission of proposals:**
- **Expected start of contract:**

TABLE OF CONTENTS

I. Introduction

Nonviolent Peaceforce (NP) NP is an international non-governmental organization reimagining security and civilian protection in areas most impacted by instability and conflict by working alongside communities to interrupt and prevent violence. Grounded in values of nonviolence, NP radically centers those most impacted by violence, to enable people to be able to directly enhance their security and dignity through Unarmed Civilian Protection (UCP). NP envisions a world where through the use of UCP and other nonviolent tactics, our collective capacity for collaboration over competition will be strengthened.

Nonviolent Peaceforce is seeking an ICT service provider to develop and implement cohesive tech support for our international operations. We are searching for a tech company for humans, a service-oriented, values driven company who can partner with us to facilitate technical efficiency, reducing risk exposure through strengthening cyber security and contributing to NP's business continuity capacity.

Currently, NP has 9 country programmes, a global headquarters and regional representation across the regions of Africa, Asia, Middle East, Europe and North America.

More information on the services required are detailed in section II.

II. Mandate overview

NP has approximately 350 employees, with an estimated 500 devices (laptops & mobile phones), operating across 10+ countries. ICT services have been semi centralized through shared platform tools (Salesforce, BambooHR, Office 365) with help desk services split between geographically proximate service providers and a central "HQ" driven service.

The main services required are:

Hardware & Software Support:
- Device audit (laptops), assess capacities and develop rolling investment plan for maintenance and performance
- Verify existing licences at headquarters (HQ) & in country offices to ensure that there are no duplicates or other separate licences. Ideally, NP wants to obtain the same operating licences for all its offices.
- Improve current backup practices and verify that backups are done regularly. Propose alternative backup models adapted to NP's context and in line with current best practices.

Help Desk & Tech Training
- Rapid response for tech problems across multiple time zones
- Regular "fake" phishing exercises to assess awareness of NP staff across teams.
- Skills building training sessions

Network Infrastructure Management

Configuration Management

- Device Configuration: Setting up routers, switches, firewalls, and other network devices to ensure correct communication paths, policies, and security settings.
- Standardization: Maintaining consistent configurations across similar devices for easier management, troubleshooting, and compliance.
- Automation and Scripting: Using automation tools to apply bulk configurations, implement updates, and manage settings at scale.

Fault Management and Troubleshooting

- Incident Detection and Response: Quickly identifying, isolating, and resolving faults or outages that affect network operations.
- Root Cause Analysis: Investigating the underlying reasons for network issues to prevent recurrence.
- Incident Documentation: Recording details of incidents, troubleshooting steps, and resolutions to improve response to similar future events.

Security Management

- Network Access Control: Restricting access to network resources based on user identity, device type, and location.
- Threat Detection and Mitigation: Identifying and responding to threats such as DDoS attacks, malware, and unauthorized access attempts.
- Patch and Vulnerability Management: Regularly updating network devices with security patches and monitoring for vulnerabilities.
- Data Encryption and Privacy: Ensuring secure data transmission across the network, especially for customer data, through encryption and secure protocols.

Disaster Recovery and Business Continuity Planning

- Backup and Restoration: Regularly backing up configurations, logs, and critical data to ensure recovery in case of a disaster.
- Disaster Recovery Planning: Developing and testing a plan to restore network services quickly after a major disruption.
- Redundancy and Geodiversity: Using geographically dispersed data centers and redundant systems to minimize the impact of localized disruptions.

Policy and Compliance Management

- **Policy Enforcement**: Ensuring that network configurations and usage comply with organizational policies and regulatory standards.
- **Regulatory Compliance**: Adhering to industry regulations such as GDPR, HIPAA, or local telecommunications laws, which may include data protection, reporting, and auditing.
- **Documentation and Auditing**: Keeping accurate records of network configurations, changes, incidents, and compliance checks for accountability and regulatory requirements.

III. Selection criteria and required qualifications

The Provider must display sufficient experience by having successfully completed other similar projects.
The proposal must contain a detailed budget calculation, detailing the hourly costs for conducting all the work required.

The Provider will be selected based upon:

- Technical suitability and proficiency (55 points): demonstrable expertise and experience of sufficient resources.
- The most value for money (25 points).

Additional selection criteria:

- Record of corporate social responsibility (CSR) initiatives (20 points).

- The Provider must disclose where their servers and storage of data is located and disclose the source of the energy mix used in the country of data storage.

- NP strongly believes in gender equity. Please provide details on no. of women in leading positions in the company.

IV. Timeframe and procedures

Prospective providers should submit a full proposal referencing the items above and specifically outlining their capacity to fulfil the Mandate as presented in section II. Deadline for submissions:

The following timeline applies to this procedure:

1.	Call for proposals officially announced	December 3, 2024
2.	Deadline for receiving proposals	January 20, 2025
3.	Final selection of company	February 20, 2025

V. Budget and payment modalities

The payment modalities will be established upon the start of the contract and shall be in line with NP's own rules and procedures. Payments will be made against a detailed invoice, within a period of 30 days from the date of invoice submission. The contract is subject to NP's terms of business.

VI. Submission of proposals

Please submit the offer by email to **tenders@nonviolentpeaceforce.org** . Mention the title of this call for proposals (see first page) in the subject line of your offer email.

It is essential that the proposal includes the following elements:

- Proof of legal registration.
- A short presentation of the company and team, including CVs of senior team.
- A list of similar successful past projects outlining the company's track record.
- The technical and financial offer in English, with detailed responses to sections II & III of this call for proposals, detailing monthly costs of maintenance and support services, as well as development services, and any additional charges and/or deductions. The monthly costs should be articulated by estimated number of devices.
- References from previous partners (especially if they are NGOs) are welcome and will be required before entering any contractual relationship with NP.