Terms of Reference (ToR)-IT Security Audit of NAPP IT Applications

1. Background

Fairtrade NAPP supports and empowers Fairtrade certified farmers and workers across the Asia Pacific region. The producers share a 50% ownership of the Fairtrade system and have an equal voice in all decisions that affect them. Currently, NAPP has 300+ Producer Organizations across 21 countries in Asia and the Pacific Region, supporting more than 260000 farmers and workers. Fairtrade strengthens the position of farmers and workers in the value chain. By offering an alternative approach to trade, NAPP supports producers in securing better markets, contributing to greater sustainable development in the Asia Pacific region under Fairtrade – Network of Asia and Pacific Producers (NAPP). To know more about NAPP & Fairtrade visit: https://www.fairtradenapp.org, https://www.fairtrade.net

NAPP relies on a suite of IT applications to manage producer data, facilitate compliance monitoring, support internal operations, and enable communication with stakeholders.

Given the increasing risks of cyber threats, data breaches, and regulatory requirements, NAPP seeks to strengthen its IT security posture. This audit will provide an independent assessment of vulnerabilities, risks, and compliance gaps, ensuring that NAPP's IT systems remain secure, resilient, and aligned with international best practices.

2. Purpose of the Assignment

The purpose of this assignment is to conduct a **comprehensive IT Security Audit** of NAPP's IT applications. The audit will:

- Identify vulnerabilities and risks across applications and infrastructure.
- Assess compliance with relevant standards and regulations (ISO 27001, GDPR, local data protection laws).
- Recommend corrective and preventive measures to enhance IT security.
- Provide management with a clear roadmap for strengthening IT resilience.

3. Scope of Work

The auditor/firm will undertake the following tasks:

- **Application Security Review**: Analyze architecture, configurations, and deployment of NAPP's IT applications.
- **Vulnerability Assessment & Penetration Testing**: Conduct controlled tests to identify exploitable weaknesses.
- **Access Control & Authentication**: Review user roles, privileges, and authentication mechanisms.
- **Data Protection & Privacy**: Assess encryption, data storage, and compliance with

GDPR and local laws.

- **Network & Infrastructure Security**: Evaluate firewalls, VPNs, and server configurations.
- **Backup & Disaster Recovery**: Review policies and test recovery procedures.
- **Incident Response Readiness**: Assess protocols for detecting, reporting, and responding to security incidents.
- **Policy & Compliance Review**: Benchmark against ISO 27001, SOC2, and other relevant frameworks.

4. Deliverables

The auditor/firm will provide:

- **Comprehensive Audit Report**: Detailed findings, risk ratings, and identified vulnerabilities.
- **Recommendations & Action Plan**: Practical steps for remediation and long-term improvements.
- **Executive Summary**: Concise overview for senior management highlighting critical risks.
- **Presentation of Findings**: Formal briefing to NAPP leadership and IT team.

5. Duration & Timeline

- The assignment will be completed within **4 weeks** of contract signing.
- Weekly progress updates will be shared with NAPP's IT Manager.
- Final report and presentation must be delivered by the end of Week 4.

6. Budget & Payment Terms

- The total contract value is **€2000 (Two Thousand Euros)**.
- This amount is inclusive of all professional fees, taxes, and expenses.
- Payment will be made in two tranches:
    - 50% upon signing of contract.
    - 50% upon submission of the final report and presentation.

7. Eligibility Criteria

Applicants must demonstrate:

- Proven experience in IT security audits of enterprise applications.
- Familiarity with compliance frameworks (ISO 27001, GDPR, SOC2).
- Availability of certified professionals (CISSP, CEH, CISA preferred).
- Ability to deliver within the stipulated timeline.
- Strong references from similar assignments.

8. Reporting & Coordination

- The auditor will report directly to the **NAPP IT Manager**.
- Coordination with application owners, IT staff, and relevant stakeholders will be required.
- Confidentiality agreements must be signed prior to commencement.

9. Proposal Submission

Interested firms/individuals are invited to submit:

- **Technical Proposal**: Methodology, tools, and audit approach.
- **Profile of Key Personnel**: Qualifications and certifications.
- **Relevant Past Experience**: Evidence of similar assignments.
- **Financial Proposal**: Confirmation of acceptance of the €2000 budget.

10. Confidentiality & Ethics

All information accessed during the audit will be treated as strictly confidential. The auditor must adhere to ethical standards, ensuring no data is disclosed or misused.

11. Application:

- Please provide a brief expression of interest highlighting your experience and understanding of the project with other similar applications.
- Kindly submit a comprehensive budget proposal.
- **Deadline:** Send your EOI and budget to gideon.balasingam@fairtradenapp.org by Sept 20, 2026.